L Number	Hits	Search Text	DB	Time stamp
1	1	("6041316").PN.	USPAT; US-PGPUB	2003/08/04 16:01
2	1	("6105012").PN.	USPAT; US-PGPUB	2003/08/04 16:02
3	1	("5303303").PN.	USPAT; US-PGPUB	2003/08/04 16:03
4	1	("5729594").PN.	USPAT; US-PGPUB	2003/08/04 16:04
-	145	(713/151).CCLS.	USPAT; US-PGPUB	2003/07/29 07:49
-	13	(US-6353886-$ or US-6334186-$ or US-5671279-$ or US-6058482-$ or US-6105012-$ or US-5870544-$ or US-5825890-$).did. or (US-20030018887-$ or US-20030005283-$ or US-20020146128-$ or US-20020032853-$ or US-20010023482-$ or US-20010009025-$).did.	USPAT; US-PGPUB	2003/07/28 13:06
-	0	((713/151).CCLS.) and (tcp/ip SAME java)	USPAT; US-PGPUB	2003/07/28 11:53
-	49	((713/151).CCLS.) and tcp/ip	USPAT; US-PGPUB	2003/07/28 11:53
-	11	(((713/151).CCLS.) and tcp/ip) and java	USPAT; US-PGPUB	2003/07/28 11:53
-	116	(713/160).CCLS.	USPAT; US-PGPUB	2003/07/29 10:12
-	4	(US-6055314-$ or US-6247130-$).did. or (US-20010010720-$ or US-20030068046-$).did.	USPAT; US-PGPUB	2003/07/28 14:16
-	3	("5991399" | "6009410" | "6038595").PN.	USPAT	2003/07/28 13:32
-	1	6247130.URPN.	USPAT	2003/07/28 13:33
-	14	("4736422" | "4908834" | "5029207" | "5054064" | "5420866" | "5481609" | "5539828" | "5640453" | "5644354" | "5666412" | "5721778" | "5721781" | "5742756" | "5745571").PN.	USPAT	2003/07/28 13:35
-	131	(713/166).CCLS.	USPAT; US-PGPUB	2003/07/28 13:37
-	1	("6105012").PN.	USPAT; US-PGPUB	2003/07/28 14:25
-	9	("5319710" | "5509071" | "5671279" | "5751813" | "5809144" | "5848161" | "5862325" | "5890171" | "5897622").PN.	USPAT	2003/07/28 14:16
-	2	6105012.URPN.	USPAT	2003/07/28 14:22
-	9	("5319710" | "5509071" | "5671279" | "5751813" | "5809144" | "5848161" | "5862325" | "5890171" | "5897622").PN.	USPAT	2003/07/28 14:23
-	1256	(client same server) and (tcp/ip same html)	USPAT; US-PGPUB	2003/07/28 14:27
-	377	((client same server) and (tcp/ip same html)) and encrypt$3	USPAT; US-PGPUB	2003/07/28 14:29
-	176	(((client same server) and (tcp/ip same html)) and encrypt$3) and (web same java)	USPAT; US-PGPUB	2003/07/28 14:30
-	108	((((client same server) and (tcp/ip same html)) and encrypt$3) and (web same java)) and packet	USPAT; US-PGPUB	2003/07/28 14:31
-	3	(US-5729594-$).did. or (US-20020188513-$ or US-20020032725-$).did.	USPAT; US-PGPUB	2003/07/28 15:39
-	159	(encrypt$3 same non-encrypt$3) and (client same server)	USPAT; US-PGPUB	2003/07/28 15:47
-	24	((encrypt$3 same non-encrypt$3) and (client same server)) and (web same java)	USPAT; US-PGPUB	2003/07/28 15:48
-	1	("0000200").PN.	USPAT; US-PGPUB	2003/07/29 07:49
-	1736	(713/200).CCLS.	USPAT; US-PGPUB	2003/07/29 07:49

-	0	("L2and(clientsameserver)").PN.	USPAT; US-PGPUB	2003/07/29 07:50
-	484	((713/200).CCLS.) and (client same server)	USPAT; US-PGPUB	2003/07/29 07:51
-	28	(((713/200).CCLS.) and (client same server)) and (tcp/ip same http same https)	USPAT; US-PGPUB	2003/07/29 16:30
-	698	(713/176).CCLS.	USPAT; US-PGPUB	2003/07/29 08:47
-	0	("l1and(clientsameserver)").PN.	USPAT; US-PGPUB	2003/07/29 08:47
-	127	((713/176).CCLS.) and (client same server)	USPAT; US-PGPUB	2003/07/29 08:47
-	23	(((713/176).CCLS.) and (client same server)) and tcp/ip	USPAT; US-PGPUB	2003/07/29 08:48
-	0	("l10and(selectiveADJencrypt$3)").PN.	USPAT; US-PGPUB	2003/07/29 10:13
-	0	((713/160).CCLS.) and (selectiveADJencrypt$3)	USPAT; US-PGPUB	2003/07/29 10:13
-	116	(713/160).CCLS.	USPAT; US-PGPUB	2003/07/29 12:12
-	1	("5159630").PN.	USPAT; US-PGPUB	2003/07/29 12:15
-	1	("6041316").PN.	USPAT; US-PGPUB	2003/07/29 12:17
-	1	("5361256").PN.	USPAT; US-PGPUB	2003/07/29 12:18
-	1	("4172213").PN.	USPAT; US-PGPUB	2003/07/29 12:19
-	1	("5325432").PN.	USPAT; US-PGPUB	2003/07/29 12:20
-	1	("5832212").PN.	USPAT; US-PGPUB	2003/07/29 12:22
-	1	("5960080").PN.	USPAT; US-PGPUB	2003/07/29 12:25
-	0	("(clientsameserver)or(transmit$3samereceiv$3").PN.	USPAT; US-PGPUB	2003/07/29 12:26
-	341802	(client same server) or (transmit$3 same receiv$3)	USPAT; US-PGPUB	2003/07/29 16:27
-	14	(((client same server) or (transmit$3 same receiv$3)) and (partial ADJ encrypt$3) or (selective ADJ encrypt$3)) and tcp/ip	USPAT; US-PGPUB	2003/07/29 12:28
-	87	((client same server) or (transmit$3 same receiv$3)) and (partial ADJ encrypt$3) or (selective ADJ encrypt$3)	USPAT; US-PGPUB	2003/07/29 15:19
-	330	"4200770"	USPAT; US-PGPUB	2003/07/29 15:19
-	1	("4200770").PN.	USPAT; US-PGPUB	2003/07/29 15:20
-	1	("4405289").PN.	USPAT; US-PGPUB	2003/07/29 15:21
-	1	("4405829").PN.	USPAT; US-PGPUB	2003/07/29 16:02
-	1	("5832212").PN.	USPAT; US-PGPUB	2003/07/29 16:07
-	1	("5946467").PN.	USPAT; US-PGPUB	2003/07/29 16:12
-	1	("6415031").PN.	USPAT; US-PGPUB	2003/07/29 16:14
-	1	("6229895").PN.	USPAT; US-PGPUB	2003/07/29 16:19
-	1	("6415031").PN.	USPAT; US-PGPUB	2003/07/29 16:19
-	298	((client same server) or (transmit$3 same receiv$3)) and (tcp/ip same java) and packet	USPAT; US-PGPUB	2003/07/29 16:28
-	298	(((client same server) or (transmit$3 same receiv$3)) and (tcp/ip same java) and packet) and java	USPAT; US-PGPUB	2003/07/29 16:30

-	0	(((client same server) or (transmit$3 same receiv$3)) and (tcp/ip same java) and packet) and (partial ADJ encrypt$3)	USPAT; US-PGPUB	2003/07/29 16:31
-	231	(((client same server) or (transmit$3 same receiv$3)) and (tcp/ip same java) and packet) and http	USPAT; US-PGPUB	2003/07/29 16:31
-	163	(((client same server) or (transmit$3 same receiv$3)) and (tcp/ip same java) and packet) and encrypt$3	USPAT; US-PGPUB	2003/07/29 16:32
-	137	((((client same server) or (transmit$3 same receiv$3)) and (tcp/ip same java) and packet) and encrypt$3) and http	USPAT; US-PGPUB	2003/07/29 16:32
-	1	("5671279").PN.	USPAT; US-PGPUB	2003/07/30 11:20
-	1	("5126728").PN.	USPAT; US-PGPUB	2003/07/30 11:22
-	116	(713/160).CCLS.	USPAT; US-PGPUB	2003/07/31 09:23
-	0	("12andpacket").PN.	USPAT; US-PGPUB	2003/07/30 13:44
-	83	((713/160).CCLS.) and packet	USPAT; US-PGPUB	2003/07/31 10:57
-	13	(US-6460137-$ or US-5442708-$ or US-5444782-$ or US-5594869-$ or US-5640456-$ or US-6240514-$ or US-4661657-$ or US-4910777-$ or US-5706348-$ or US-5805705-$ or US-5825888-$ or US-5870479-$ or US-5228083-$).did.	USPAT	2003/07/31 12:30
-	34	"5081678"	USPAT; US-PGPUB	2003/07/30 15:20
-	1	("5081678").PN.	USPAT; US-PGPUB	2003/07/30 15:20
-	1	("5050213").PN.	USPAT; US-PGPUB	2003/07/30 16:28
-	1	("6041316").PN.	USPAT; US-PGPUB	2003/07/30 16:28
-	5	6041316.URPN.	USPAT	2003/07/30 16:32
-	1	("6041316").PN.	USPAT; US-PGPUB	2003/07/31 08:32
-	11	("4658093" | "4740890" | "4817140" | "4827508" | "5014234" | "5050213" | "5237614" | "5265164" | "5321520" | "5341429" | "5457746").PN.	USPAT	2003/07/31 08:33
-	117	(713/160).CCLS.	USPAT; US-PGPUB	2003/07/31 09:23
-	84	((713/160).CCLS.) AND PACKET	USPAT; US-PGPUB	2003/07/31 09:23
-	1	(((713/160).CCLS.) AND PACKET) and cookie	USPAT; US-PGPUB	2003/07/31 10:02
-	49	"5987611"	USPAT; US-PGPUB	2003/07/31 10:02
-	1	("5987611").PN.	USPAT; US-PGPUB	2003/07/31 10:02
-	76	(((713/160).CCLS.) AND PACKET) and encrypt$3	USPAT; US-PGPUB	2003/07/31 10:58
-	14	((((713/160).CCLS.) AND PACKET) and encrypt$3) and (client same server)	USPAT; US-PGPUB	2003/07/31 10:58
-	4	("2304499").PN.	USPAT; US-PGPUB; DERWENT	2003/07/31 13:17
-	0	("200120032903").PN.	USPAT; US-PGPUB; DERWENT	2003/07/31 13:18
-	2	("20020032903").PN.	USPAT; US-PGPUB; DERWENT	2003/07/31 14:20
-	2	("5126728").PN.	USPAT; US-PGPUB; DERWENT	2003/07/31 14:27

-	382	((client same server) and (tcp/ip same html)) and encrypt$3	USPAT; US-PGPUB	2003/07/31 14:32
-	326	(((client same server) and (tcp/ip same html)) and encrypt$3) and key	USPAT; US-PGPUB	2003/07/31 14:32
-	322	((((client same server) and (tcp/ip same html)) and encrypt$3) and key) and form	USPAT; US-PGPUB	2003/07/31 14:33
-	189	(((((client same server) and (tcp/ip same html)) and encrypt$3) and key) and form) and packet	USPAT; US-PGPUB	2003/07/31 14:33
-	123	((((((client same server) and (tcp/ip same html)) and encrypt$3) and key) and form) and packet) and java	USPAT; US-PGPUB	2003/07/31 15:02
-	1594	(e adj commerce) and (encrypt$3)	USPAT; US-PGPUB	2003/07/31 15:03
-	1001	((e adj commerce) and (encrypt$3)) and (client same server)	USPAT; US-PGPUB	2003/07/31 15:03
-	50	(((e adj commerce) and (encrypt$3)) and (client same server)) and (tcp/IP same java)	USPAT; US-PGPUB	2003/07/31 15:04
-	46	((((e adj commerce) and (encrypt$3)) and (client same server)) and (tcp/IP same java)) and key	USPAT; US-PGPUB	2003/07/31 15:11
-	100	((713/160).CCLS.) and key	USPAT; US-PGPUB	2003/07/31 15:12
-	22	(((713/160).CCLS.) and key) and (client same server)	USPAT; US-PGPUB	2003/07/31 15:12
-	1	("5671279").PN.	USPAT; US-PGPUB	2003/08/04 15:59

```
File 696:DIALOG Telecom. Newsletters 1995-2003/Jul 30
         (c) 2003 The Dialog Corp.
File  15:ABI/Inform(R) 1971-2003/Jul 31
         (c) 2003 ProQuest Info&Learning
File  98:General Sci Abs/Full-Text 1984-2003/Jun
         (c) 2003 The HW Wilson Co.
File 484:Periodical Abs Plustext 1986-2003/Jul W4
         (c) 2003 ProQuest
File 553:Wilson Bus. Abs. FullText 1982-2003/Jun
         (c) 2003 The HW Wilson Co
File 813:PR Newswire 1987-1999/Apr 30
         (c) 1999 PR Newswire Association Inc
File 613:PR Newswire 1999-2003/Jul 31
         (c) 2003 PR Newswire Association Inc
File 635:Business Dateline(R) 1985-2003/Jul 31
         (c) 2003 ProQuest Info&Learning
File 810:Business Wire 1986-1999/Feb 28
         (c) 1999 Business Wire
File 610:Business Wire 1999-2003/Jul 31
         (c) 2003 Business Wire.
File 369:New Scientist 1994-2003/Jul W3
         (c) 2003 Reed Business Information Ltd.
File 370:Science 1996-1999/Jul W3
         (c) 1999 AAAS
File  20:Dialog Global Reporter 1997-2003/Jul 31
         (c) 2003 The Dialog Corp.
File 624:McGraw-Hill Publications 1985-2003/Jul 31
         (c) 2003 McGraw-Hill Co. Inc
File 634:San Jose Mercury  Jun 1985-2003/Jul 30
         (c) 2003 San Jose Mercury News
File 647:CMP  Computer Fulltext 1988-2003/Jul W1
         (c) 2003 CMP Media, LLC
File 674:Computer News Fulltext 1989-2003/Jul W4
         (c) 2003 IDG Communications
? ds

Set     Items   Description
S1    3268045   KEY? ? OR CIPHER? OR CYPHER? OR ALGORITHM?
S2     167412   S1(3N)(SEND??? ? OR SENT OR TRANSMIT? OR TRANSMIS? OR TRAN-
              SFER? OR XFER? OR DELIVER? OR ISSUE? ? OR ISSUING OR ISSUANCE?
               OR RECEIV? OR RECEIPT? ? OR RECEPTION?)
S3     356447   CIPHER? OR CYPHER? OR ENCIPHER? OR ENCYPHER? OR ENCRYPT? OR
              SCRAMBL? OR ENCOD???? ?
S4      54772   S3(3N)(DATA OR INFORMATION OR PACKET? ? OR MESSAG??? ? OR -
              FILE OR FILES OR CONTENT)
S5       4959   S4(3N)(USER? OR CLIENT? OR RECIPIENT? OR BUYER? OR RECEIVE-
              R? OR PATRON? OR PURCHASER? OR CONSUMER? OR CUSTOMER? OR SHOP-
              PER? OR SUBSCRIBER?)
S6        128   S4(3N)(REQUEST?R? ? OR ESHOPPER? OR PARTICIPANT? OR MEMBER?
               ? OR NETIZEN?)
S7        541   S4(3N)(INDIVIDUAL? ? OR PERSON? ? OR PARTY)
S8        565   S2 AND S5:S7
S9       5537   S2(3N)(USER? ? OR CLIENT? OR RECIPIENT? OR BUYER? OR PATRO-
              N? OR PURCHASER? OR CONSUMER? OR CUSTOMER? OR SHOPPER? OR SUB-
              SCRIBER?)
S10      2360   S2(3N)(REQUEST?R? ? OR ESHOPPER? OR PARTICIPANT? OR MEMBER?
               ? OR NETIZEN? OR INDIVIDUAL? ? OR PERSON? ? OR PARTY)
S11       287   S2(S)S5:S7
S12        86   S10(S)S8:S9
S13       190   S9:S10(S)S4
S14      1740   UNENCRYPT? OR UNENCIPHER? OR UNENCYPHER? OR UNCRYPT? OR UN-
```

```
            CYPHER? OR UNCIPHER? OR NONCRYPT? OR NONCIPHER? OR NONCYPHER?
            OR NONSCRAMBL?
S15         58   NONENCRYPT? OR NONENCIPHER? OR NONENCYPHER?
S16        246   (NON OR UN)()(ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR CRYPT?
            OR CYPHER? OR CIPHER? OR ENCOD????)
S17        171   NONENCOD? OR UNENCOD?
S18       2887   (S3 OR S14:S17)(3N)(PARTIAL? OR PARTLY OR PART OR PARTS OR
            PORTION? OR SECTION? ? OR SEGMENT? ?)
S19         71   S11(S)S9:S10
S20          4   S13(S)S18
S21          0   S19(S)S18
S22          0   S11(S)S18
S23         21   S18(S)S2
S24         25   S18(S)S5:S7
S25          7   S18(S)S9:S10
S26        185   S12 OR S19:S25
S27         77   S26/2000:2003
S28        108   S26 NOT S27
S29         89   RD (unique items)
? t29/3,k/6,20
```

29/3,K/6 (Item 4 from file: 15)

DIALOG(R)File 15:ABI/Inform(R)

01917463 05-68455

Reel to real: Should you believe what you see?

Harts, Dean M

Defense Counsel Journal v66n4 PP: 514-524 Oct 1999
ISSN: 0895-0016 JRNL CODE: ISC
WORD COUNT: 6658

...TEXT: or encrypt the data file; the second is used to verify the signature or de- **encrypt** the **data file** .

Each **party** using digital signatures has a "public key" and a "private key." The public key is openly distributed; the private key is kept confidential. The person who **encrypts** a digital **message** uses the **recipient** 's public **key** and **sends** the message. Now, only the recipient's private key can decipher the message, and anyone...

... the message cannot read it. Thus, the sender and recipient need not share any confidential **key** , and each can **send** and receive secure digital messages."

B. Use Hash Marks
Another option involves running a data...

29/3,K/20 (Item 18 from file: 15)

DIALOG(R)File 15:ABI/Inform(R)

01317326 99-66722

Security, anonymity and digital currencies

Anonymous

Telecommunications (International Edition) v30n10 PP: 90 Oct 1996
ISSN: 0040-2494 JRNL CODE: TIE
WORD COUNT: 227

...TEXT: entity can duplicate. The receiver of such a message can only decrypt it with the **sender** 's **key** . Using such keys successfully authenticates that the message was from the real sender. Another approach involves **encrypting** **part** of a message with the same public key, and appending it to the message being...
? t29/3,k/22,26,40

29/3,K/22 (Item 20 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01281554 99-30950
The key to security
Bort, Julie
InfoWorld v18n36 PP: 1, 51+ Sep 2, 1996
ISSN: 0199-6649 JRNL CODE: IFW
WORD COUNT: 2273

...TEXT: key stored somewhere that is available. Should someone want to send an encrypted message, the **sender** locates the public **key** of the **recipient** , **encodes** the **message** , and sends it off. The receiver then uses a private key to decode the message...

29/3,K/26 (Item 24 from file: 15)
DIALOG(R)File 15:ABI/Inform(R)

01004374 96-53767
Encryption systems use two keys
Anonymous
InfoWorld v17n12 PP: 44 Mar 20, 1995
ISSN: 0199-6649 JRNL CODE: IFW
WORD COUNT: 228

...TEXT: in conjunction with the algorithm to encrypt data. A pair of keys are used to **encrypt** and decrypt **messages** .

A **user** retains a private decryption key and publishes a public encryption key, called the public key, for use by anyone interested in sending the **user** sensitive information.

Senders use **recipients** ' public **keys** to **send** **encrypted** **messages** . **Recipients** use their corresponding private keys to decrypt messages.

A digital signature verifies the identity of...

29/3,K/40 (Item 3 from file: 553)
DIALOG(R)File 553:Wilson Bus. Abs. FullText

03061470 H.W. WILSON RECORD NUMBER: BWBA95061470 (USE FORMAT 7 FOR FULLTEXT)
Doing business on the Internet--a question of balance.
Arnum, Eric
Business Communications Review (Bus Commun Rev) v. 25 (Aug. 1995) p. 35-7
LANGUAGE: English
WORD COUNT: 2754

(USE FORMAT 7 FOR FULLTEXT)

TEXT:
... the listed sender and that it is unchanged from the original.
Privacy: A sender can **encrypt** a **message** with the **recipient** 's public key, which can be obtained from an agreed on source such as a common directory, a key management system or even the **recipient** . Only the **receiver** 's private **key** can decrypt the message, and there might also be a digital signature within the envelope...
? t29/3,k/59,62,64,75

29/3,K/59 (Item 4 from file: 810)
DIALOG(R)File 810:Business Wire

0651698 BW1152

SCHLUMBERGER: Schlumberger launches industry's most secure smart card; Cryptoflex delivers exceptional speed and security for authorizing transactions

December 05, 1996

Byline: Business/High-Tech Editors

...yet developed. A message
sent from one person to another can be secured by first **encrypting** the message with the **recipient** 's public **key** , **transmitting** the message,
and decrypting the message with the recipient's private key. With a key...

29/3,K/62 (Item 1 from file: 369)
DIALOG(R)File 369:New Scientist

00103963 14519654.200 (USE FORMAT 7 OR 9 FOR FULLTEXT)
Publish and Be Robbed?: Distributing your work on the Internet may seem like the best way to reach a wide audience. But can musicians, photographers and publishers repel the digital pirates?
LAURENCE, ANDY; FREELANCE WRITER SPECIALISING IN TECHNOLOGY AND BUSINESS ISSUES
New Scientist, vol. 145, no. 1965, p. Page 32
February 18, 1995
LANGUAGE: English RECORD TYPE: Fulltext DOC. TYPE: Journal
WORD COUNT: 3384

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:
...which is free to anyone with access to the Internet, uses two keys: the public **key** which the **person sending** the **information** uses to **encode** the confidential material and the separate private key which decodes the message. The person receiving...

29/3,K/64 (Item 2 from file: 20)
DIALOG(R)File 20:Dialog Global Reporter

06344603 (USE FORMAT 7 OR 9 FOR FULLTEXT)
Digital signatures: Present and future
BUSINESS LINE
July 23, 1999
JOURNAL CODE: FBLN LANGUAGE: English RECORD TYPE: FULLTEXT
WORD COUNT: 814

(USE FORMAT 7 OR 9 FOR FULLTEXT)

... key to individuals. Information that is to be encrypted is done so using the private **key** . The **individual** then **sends** the **encrypted data** to the addressee, say, a retailer. Along with the encrypted data, the sender also **sends** the public **key** assigned to him. (The public key will also be available in directories in the Internet...

29/3,K/75 (Item 1 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext
(c) 2003 CMP Media, LLC. All rts. reserv.

01168997 CMP ACCESSION NUMBER: LTH19980801S0032
Blanket Security (Drivers)
David Ticoll
TELE.COM, 1998, n 309, PG46
PUBLICATION DATE: 980801
JOURNAL CODE: LTH LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Voices
WORD COUNT: 1134

... essence, each PKI user possesses a two-part key-a public part and a private **part** . Data **encrypted** with the public key can only be decrypted using the associated private key, which its...

...the public key to anyone with whom he or she wishes to communicate. A sender **encrypts** a **message** using the **recipient** 's public key, and the recipient uses a private key to decrypt the message. Every...
? t29/3,k/78,82-83,87,89

29/3,K/78 (Item 4 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext
(c) 2003 CMP Media, LLC. All rts. reserv.

01124192 CMP ACCESSION NUMBER: EET19970428S0107
Data security chips ward off intrusions
Richard Takahashi, Director of Engineering, Secure and Commercial Products Group, VLSI Technology Inc., San Jose, Calif.
ELECTRONIC ENGINEERING TIMES, 1997, n 951, PG98
PUBLICATION DATE: 970428
JOURNAL CODE: EET LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Embedded Systems
WORD COUNT: 1758

... algorithms to commercial use. Public-key algorithms do not rely on the same key to **encrypt** and decrypt operations. Message transmitter and **receiver** hold different **keys** . To **send** a message, the transmitter and **receiver** exchange their **keys** . The message **transmitter** combines his or her key with the **recipient** 's private **key** and **sends** the

message. Public- **key** algorithms do not require both keys to be secret or private. Only one of the...

29/3,K/82 (Item 8 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01057816 CMP ACCESSION NUMBER: IAA19950703S0048
Key technology (Briefs)
INTERACTIVE AGE, 1995, n 218, PG32
PUBLICATION DATE: 950703
JOURNAL CODE: IAA LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Electronic Commerce
WORD COUNT: 83

TEXT:
Public key cryptography uses a matched pair of public and private **keys** . To **send** a **message** , an **individual** **encrypts** the **message** with the intended **recipient** 's public key. Once encrypted, the message can be decrypted only with the recipient's...

29/3,K/83 (Item 9 from file: 647)
DIALOG(R)File 647:CMP Computer Fulltext

01018008 CMP ACCESSION NUMBER: CWK19940620S1109
Start-Up to Develop Security Kits
SHARON FISHER
COMMUNICATIONSWEEK, 1994, n 510, 39
PUBLICATION DATE: 940620
JOURNAL CODE: CWK LANGUAGE: English
RECORD TYPE: Fulltext
SECTION HEADING: Network Mangement
WORD COUNT: 566

... they cannot be read by other users.
RSA's software uses public-key cryptography to **encrypt** **messages** and authenticate **users** sending them. The technology is based on public **keys** , which let the **sender** and **recipient** exchange **encrypted** **messages** without exchanging **encryption** keys first.
Terisa will develop two classes of tool kits, the partners said. The SecureWeb...

29/3,K/87 (Item 3 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

069166
No forgeries on this Web
Byline: Mark Gibbs
Journal: Network World Page Number: 15
Publication Date: September 28, 1998
Word Count: 789 Line Count: 70

Text:
... is a checksum of the document's contents, using a special utility that

is often **part** of a message- **encryption** system. The checksum is called a digest because it takes arbitrary data and produces a...

... private key that only the owner has. To send a message using this method, you **encrypt** the **data** using the **recipient** 's public key. When the recipient gets the message, he uses his private key to...

29/3,K/89 (Item 5 from file: 674)
DIALOG(R)File 674:Computer News Fulltext

004136
A network security primer
OSI guidelines can help you plan and build more secure systems
Byline: William Stallings; Stallings is President of Comp-Comm Consulting in Prides Crossing, Mass., and author of 14 books on data communications.
Journal: Computerworld Page Number: 63
Publication Date: January 29, 1990
Word Count: 3820 Line Count: 276

Text:
...end-to-end encryption are needed.
When both forms of encryption are employed, the host **encrypts** the **user - data portion** of a packet using an end-to-end encryption key. The entire packet is then...

File 256:SoftBase:Reviews,Companies&Prods. 82-2003/Jun
(c)2003 Info.Sources Inc
? ds

Set	Items	Description
S1	2765	CIPHER? OR CYPHER? OR ENCIPHER? OR ENCYPHER? OR ENCRYPT? OR SCRAMBL?
S2	340	DECRYPT? OR UNENCRYPT? OR UNENCIPHER? OR UNENCYPHER? OR DECIPHER? OR DECYPHER? OR UNCRYPT? OR UNSCRAMBL? OR DESCRAMBL?
S3	2	UNCYPHER? OR UNCIPHER? OR NONCRYPT? OR NONCIPHER? OR NONCYPHER? OR NONSCRAMBL? OR NONENCRYPT? OR NONENCIPHER? OR NONENCYPHER?
S4	1146	S1(3N)(DATA OR INFORMATION OR PACKET? ? OR MESSAG??? ? OR FILE OR FILES OR CONTENT)
S5	137	S2:S3(3N)(DATA OR INFORMATION OR PACKET? ? OR MESSAGE??? ? OR FILE OR FILES OR CONTENT)
S6	18075	SEND??? ? OR SENT OR TRANSMIT? OR TRANSMIS? OR TRANSFER? OR XFER? OR DELIVER?
S7	7398	SHARE? ? OR SHARING
S8	5045	RECEIV? OR RECEIPT? ? OR RECEPTION?
S9	800	BIDIRECTION? OR (TWO OR BOTH OR BI)()(WAY OR WAYS OR DIRECTION? ?) OR BACK(2N)FORTH
S10	5451	EXCHANG? OR SWAP???? ?
S11	53910	NETWORK? OR LAN OR LANS OR WAN OR WANS OR INTERNET? OR EXTRANET? OR INTRANET? OR WLAN? ? OR SUBNET? ? OR SUBNETWORK? OR VPN? ?
S12	5994	CLIENT?(2W)SERVER? ? OR CLIENT?(7N)HOST? ?
S13	29687	WEB OR WEBSITE? OR WWW OR W3 OR NET OR CYBER????? ?
S14	6022	KEY? ? OR CIPHER? OR CYPHER? OR ALGORITHM?
S15	206	S14(3N)(S6 OR S8 OR ISSUE? ? OR ISSUING OR ISSUANCE?)
S16	49	S15 AND S4
S17	41	S16 AND (S11:S13 OR WEBPAGE? OR VIRTUAL)
S18	15	S17/2000:2003
S19	26	S17 NOT S18
S20	633	ENCOD??? ?
S21	164	S20(3N)(DATA OR INFORMATION OR PACKET? ? OR MESSAG??? ? OR FILE OR FILES OR CONTENT)
S22	3	S15 AND S21
S23	1	S22/2000:2003
S24	2	S22 NOT S23
S25	28	S24 OR S19

? t25/7/all

25/7/1
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.
(c)2003 Info.Sources Inc. All rts. reserv.

01136247 DOCUMENT TYPE: Product

PRODUCT NAME: Encryption Plus Email 3.0 (136247)

PC Guardian (481718)
1133 E Francisco Blvd #D
San Rafael, CA 94901-5427 United States
TELEPHONE: (415) 459-0190

RECORD TYPE: Directory

CONTACT: Sales Department

Encryption Plus Email 3.0, offered by PC Guardian (R), is a Microsoft (R)

Outlook (R) and Lotus (R) Notes plug-in that protects e-mail communications. Encryption Plus Email 3.0 provides systems administrators with centralized recovery, password, user program configuration, and peer-to-peer key exchange management features. The product employs the AES algorithm, a 256-bit symmetric key **encrypting** and decrypting **messages** and attachments. A 233-bit public-private key algorithm protects the symmetric **key** as it is **transferred** with **messages** . **Encryption** Plus Email does not require key server, certificate authorities, or registration authorities. Key exchange, storage, and management processes are handled on workstations. The system is installed and configured quickly. It can be extended with the Decryptor Email Viewer component, which decrypts non-EXE e-mail formats.

REVISION DATE: 20030222

25/7/2

00122162 DOCUMENT TYPE: Review

PRODUCT NAMES: Extranets **(837385); Digital Certificates (840271**

TITLE: The Security Behind Secure Extranets
AUTHOR: Paget, Paul
SOURCE: Enterprise Systems Journal, v14 n12 p74(4) Dec 1999
ISSN: 1053-6566
HOMEPAGE: http://www.esj.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

Highly secure **extranets** employ technologies and strategic processes that fill in the gaps in the **extranet** configuration itself. For instance, a digital certificate, which can be called a 'passport to the **extranet** ,' is installed in the browser or on a smart card, where it authenticates the certificate holder. The digital certificate extends **extranet** access and authority to users based on their positions and their need to know; the certificate also maintains and ensures confidentiality and integrity of the data that is sent, received, and retrieved by users. Such secure systems are also more easily and effectively managed than those that simply use personal information numbers (PINs) and passwords. Secure **extranets** allow users to log on once to access authorized information, since the certificate and its foundational policies determine who logs on to what. The configuration can be changed by managers. **Network** managers always know who is conducting business and what they are doing because digital certificates track users' activity through a digital audit trail. Public key infrastructure (PKI), which is based on public key cryptography, also secures transactions over the **Internet** by using public and private components. **Messages** transported are **encrypted** with a public key and are then read by the **receiver** with a private **key** . Other superior security methods for **extranets** described are trusted parties (certification authorities) and registration authorities.

REVISION DATE: 20000430

25/7/3

DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.
(c)2003 Info.Sources Inc. All rts. reserv.

00115922 DOCUMENT TYPE: Review

PRODUCT NAMES: XCA (840548); 5C (840556)

TITLE: Big Brother Tackles Copy Protection
AUTHOR: Roth, Cliff
SOURCE: NewMedia, v9 n3 p15(1) Mar 1999
ISSN: 1060-7188
HOMEPAGE: http://www.newmedia.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

As new technologies link the **Internet** and home **networks** with many new sophisticated devices, unauthorized duplication of audio and video signals is emerging as a hot-button issue. A group of entertainment and information technology giants known as 5C, including Intel, Sony, Matsushita, Toshiba, and Hitachi, is proposing a system to control the duplication of media that will arrive in homes over **networks** . Two other corporations, Thomson (RCA) and Zenith (LG Electronics), have their own proposal called XCA. 5C proposes two-way communications between devices to exchange copy authorization keys, while XCA proposes a one-way standard. Both proposals involve **encrypted data** that can be read only by authorized devices. DVD is a **key** technology in the **issue** . Recordable DVD does not currently have copy protection, and several different standards are making compatibility on different players a problem, and may create lapses in copyright protection. MP3 **Internet** audio provides an ironic counterpoint to the entertainment industry's interests in copy protection surrounding DVD. MP3 can conceivably be replayed on analog players, thus any digital protection plans could be skirted. The same scenario could occur in the world of digital video.

REVISION DATE: 20020630

25/7/4
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.
(c)2003 Info.Sources Inc. All rts. reserv.

00110003 DOCUMENT TYPE: Review

PRODUCT NAMES: JSafe 1.1 (686719); RSA BSAFE 3.0 (595705)

TITLE: Secure Your Java Applications
AUTHOR: Finn, Mike
SOURCE: e-Business Advisor Magazine, v16 n6 pS26(4) Jun 1998
ISSN: 1098-8912
HOMEPAGE: http://www.advisor.com

RECORD TYPE: Review
REVIEW TYPE: Review
GRADE: A

JSafe 1.1 and BSafe 3.0 from RSA **Data** Security offer secure **encryption** technologies for use commercially with Java. RSA is a leader in electronic encryption products. It created the RSA Public Key algorithm, and its

technology is used in a host of **Internet** security products and protocols such as SSL, S-HTTP, and S/MIME. Netscape Navigator, Microsoft **Internet** Explorer, Quicken, and other products make use of RSA technology. RSA's JSafe is an all-Java library of importable classes that can provide cryptography functions for the application programmer. This means programmers need not worry about specific implementation of encryption **algorithms** . JSafe can support **sending** and receiving **encrypted information** nearly anywhere in a Java-based application. It is JDK 1.02 and JDK 1.1 compatible, so it easily is integrated into existing applications or applets. JSafe 1.1 includes performance enhancements, and it is more tightly integrated with BSafe. BSafe native libraries are C-based cryptography functions. Header files and static functions are used to implement BSafe 3.0. The integration between the two products means that JSafe can use existing BSafe code because it can now detect the presence of Bsafe native libraries. Those who prefer working with C over Java will want to use BSafe, but it is not as simple as JSafe for implementing routines.

REVISION DATE: 20011030

25/7/5

00105514 DOCUMENT TYPE: Review

PRODUCT NAMES: DES Triple (834785); Pretty Good Privacy (835072)

TITLE: Unlocking Key Issues **in Security**
AUTHOR: Staff
SOURCE: IEEE Software, v14 n5 p108(2) Sep/Oct 1997
ISSN: 0740-7459
HOMEPAGE: http://computer.org/softare

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

Dorothy Denning, an intrusion detection and database security expert, discusses encryption export, including the availability of Triple DES (**Data Encryption** Standard) and Pretty Good Privacy on the **Internet** and bills before Congress that affect security export. Triple DES is available from Japanese, South African, and European companies, as well. In spite of this availability, Denning says many companies want embedded encryption in full-fledged office suites and **virtual** private **networks** . Therefore, Microsoft's use of security tools in their software has a huge impact on what is used in the U.S. and elsewhere. However, the use of PGP has watered down the effects of export controls. Triple DES is an encryption method that uses three successive **encryptions** with the **Data Encryption** Standard, each with a different key. Each key can be three times longer than the standard 56-bit key. PGP is a complete system that includes **message** and **file encryption** , key management, and digital signatures. It employs the IDEA encryption algorithm, a 128-bit algorithm. The inability of U.S. companies to freely export encryption software negatively impacts their competitiveness and their ability to sell larger systems in which encryption is one component. Recently the Senate Committee on Commerce passed the Secure Public **Network** Act (S.909), which opens up exports but has many provisions for key recovery.

REVISION DATE: 20000228

25/7/6
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.
(c)2003 Info.Sources Inc. All rts. reserv.

00104232 DOCUMENT TYPE: Review

PRODUCT NAMES: Pretty Good Privacy (835072)

TITLE: Breaking The Code For Network **Security**
AUTHOR: Delmonico, Dayna
SOURCE: InternetWeek, v686 p75(4) Oct 20, 1997
ISSN: 0746-8121
HOMEPAGE: http://www.internetwk.com

RECORD TYPE: Review
REVIEW TYPE: Product Comparison
GRADE: Product Comparison, No Rating

Encryption is one of most important but least understood areas of computer security. Basically, **encryption** involves **scrambling information** in one place and unscrambling it when it reaches a destination. The unscrambling is performed with a password or a key. All kinds of things can be **encrypted** : **files** , folders, and directories, for example. With private **key** encryption, only the **sender** and **receiver** know the **key** . With public **key** encryption, **senders** and **receivers** hold a common **key** and some get an additional private key. When encryption is required for multiple users, a Certificate Authority (CA) is required. One of the most popular **encryption** schemes is the **Data Encryption** Standard (DES). DES allows the receiver and sender to use the same key for **encryption** and decryption. RSA **Data** Security created extensions to DES, the RC-4 and the RC-5 schemes, to improve security. These extensions use multiple keys and signatures as well as digital identifiers of the senders. Blowfish, once called Pretty Good Privacy or PGP, is a system where the sending and receiving computers negotiate a complex number. PGP is a very difficult encryption method to circumvent and is used for voice as well as data. E-mail security is addressed by the standard S/MIME. This standard uses a symmetrical **cipher** to **encrypt messages** and sends a digital signature with the message. Several companies listed in the extensive buyers' guide provide encryption technology.

REVISION DATE: 20000228

25/7/7
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.
(c)2003 Info.Sources Inc. All rts. reserv.

00103697 DOCUMENT TYPE: Review

PRODUCT NAMES: Puffer 3.0 Windows (622494)

TITLE: Puffer 3.0 acts as secure alternative to PGP Mail
AUTHOR: Peschel, Joe
SOURCE: InfoWorld, v19 n47 p120(1) Nov 24, 1997
ISSN: 0199-6649
HOMEPAGE: http://www.infoworld.com

RECORD TYPE: Review

REVIEW TYPE: Review
GRADE: A

Kent Briggs' Puffer 3.0, an e-mail and **file - encryption** package, is rated very good overall, especially for it stability and use of public- and private-key encryption; secure-wipe utility; and secret-sharing message recovery method. However, adding files to single-password protected archives is difficult. Puffer provides a secure alternative to Pretty Good Privacy's PGP Mail, which is the best known public key encryption program. With Puffer 3.0, users exchange public keys and **encrypt messages** with the **receiver** 's public **key** , while the **receiver** decrypts with a private key. During testing, Puffer's public-key encryption was tested first. Creating a key ring and generating the key was easy, and users can generate 512-, 1,024-, or 1,536-bit keys. A date for expiration of the key can be set, a useful feature for users who want to change a public key password often. A 1,536-bit key was created during testing, a slow process because the number generated had to have primality testing. Puffer allows users to accelerate this task if pre-generated prime numbers are used. Users can create self-extracting files for e-mail in order to use a symmetric cipher for correspondence; however, a secure method for **transmitting** the **key** is still needed. A message recovery method called secret sharing allows a company to establish multiple trustees to recover a message.

REVISION DATE: 20010330

25/7/8

00103338 DOCUMENT TYPE: Review

PRODUCT NAMES: RecoverKey (671479)

TITLE: RecoverKey Unlocks Data
AUTHOR: Phillips, Ken
SOURCE: PC Week, v14 n39 p138(2) Sep 15, 1997
ISSN: 0740-1604

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

Trusted Information Systems' RecoverKey is becoming a de facto standard in business. It offers an easy solution to situations where a company's decryption key becomes lost or unavailable due to a hardware crash. With a lost decryption key, data may be lost forever. RecoverKey keeps a spare key with an **encrypted file** in a lockbox. This strategy prevents loss of data, while also satisfying the government's goal of being able to decrypt anyone's file with legal authority. RecoverKey can recover **data** from **encrypted files** , drives, and e-mail. Several security software vendors have agreed to incorporate the technology in their own encryption products. RecoverKey addresses the problem of legal accessibility, while also addressing the problem of lost keys by adding a spare session key in a second lockbox. The spare can be decrypted only by a Key Recovery Center, which is run by the organization itself or a third party. With RecoverKey, an authorized party **transmits** the spare **key** lockbox to the Key Recovery Center, which then uses its own key to open the lockbox. The data remains safe with the owner at all times, and the session keys will not work on any other message. Each file header contains a spare key.

REVISION DATE: 20011130

25/7/9
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00102877 DOCUMENT TYPE: Review

PRODUCT NAMES: SnareNet 1.2 (670413)

TITLE: SnareNet Boasts No-Brainer Encryption
AUTHOR: Phillips, Ken
SOURCE: PC Week, v14 n35 p118(2) Aug 18, 1997
ISSN: 0740-1604

RECORD TYPE: Review
REVIEW TYPE: Review
GRADE: B

Snare **Networks** ' SnareNet 1.2 is recommended for security-centered organizations that want to encrypt their TCP/IP communications. It is rated good overall, with excellent capability. Usability, performance, interoperability, and manageability are rated good. No support is provided for some popular platforms, including Windows 3.1, but it is easy to manage and not expensive. Windows 3.1 users should look to McAfee Associates' NetCrypto. NetCrypto has more encryption algorithms out of the box, but does not automatically encrypt 100 percent of communications ports, while SnareNet does. All TCP ports are encrypted, and encryption-enabled hosts are determined on an ad hoc basis. No continuous management is required, and support is provided for third-party authentication add-ons. Sites that need more full-functioned enterprise support can turn to such products as Security First Technologies' Hannah or Northern Telecom's Entrust, each of which provides many encryption **algorithms** , digital certificates for **sender** authentication, extended management applications, token card support, and various other functions. Installation of SnareNet was easy, and its drop-in configuration routine is one of its best features. On a Solaris machine, SnareNet required some manual configuration. Using snoop on the Solaris machine showed that sessions between three test machines, including user names and passwords, were encrypted.

REVISION DATE: 20020630

25/7/10
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00102734 DOCUMENT TYPE: Review

PRODUCT NAMES: Pretty Good Privacy for Mail 4.5 Windows 95 & NT (647039)

TITLE: An Encryption Tool For Every Day
AUTHOR: Levitan, Arlan R
SOURCE: Computer Shopper, v17 n7 p392(1) Jul 1997
ISSN: 0886-0556
HOMEPAGE: http://www.computershopper.com

RECORD TYPE: Review

REVIEW TYPE: Review
GRADE: A

Pretty Good Privacy's now **Network** Associates' Pretty Good Privacy Mail 4.5 (PGP), the first real commercial product from the vendor, emphasizes many privacy matters. During testing, installation and setup needed about five minutes, and documentation is excellent. Most users will simply use the program to generate a key pair. The level of security needed is selected, and a pass phrase that allows access to the private key is assigned. Administration tools are included for use in a corporate setting, including encryption for particular groups of recipients and retraction of certified keys by security administrators. For users of Netscape Gold 3.0's mail facility or Eudora 3.0 for e-mail, PGP is transparently integrated in the mail environment. Functions needed for implementation and administration of PGP encryption appear as buttons on an existing toolbar. Two are on/off toggles for encryption and digital signatures. A separate 'execute encryption' button checks toggles' status and encrypts and digitally signs the message. The Eudora and NetScape PGP plug-ins automatically find the recipient's public key in a key ring database. A Key Management tool can be used with another button to allow public keys of recipients to be added to the key with only a few clicks of the mouse. The last PGP tool button inserts the public key at the end of a message to allow the receiver to use it to respond with an **encrypted message** that is decoded by the first **sender** 's private **key** .

REVISION DATE: 20020321

25/7/11
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00101681 DOCUMENT TYPE: Review

PRODUCT NAMES: Supply Chain Coordinator (663379); R/3 (366366); Oracle (004233); SSL (835111); SET (836281)

TITLE: E-Commerce Gets Set
AUTHOR: Radcliff, Deborah
SOURCE: Software Magazine, v17 n6 p86(5) Jun 1997
ISSN: 0897-8085
HOMEPAGE: http://www.softwaremagazine.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

PeopleSoft's Supply Chain Coordinator, SAP AG's R/3, Oracle's namesake database, Netscape Communications' Netscape Secure Sockets Layer (SSL), and Secure Electronic Transactions (SET) are products and technologies highlighted in a discussion of use of the SET encryption standard in electronic commerce. High-end vendors are seeing the possible value of the Internet as a business-to-business communications tool. For example, PeopleSoft announced Supply Chain Coordinator, which is an inter-enterprise planning tool that permits OEMs and their suppliers and customers to exchange information over the Internet. Once electronic commerce and banking are a substantial segment of the national economy, businesses transmitting money around on a well-traveled, public Internet require end-to-end network security made up of firewalls, secure gateways, cryptographic algorithms at the browser and desktop, PINs, passwords, and other security measures. SSL is a security technology that uses public key

cryptography, which **encodes** **data** with a 48- to 126-bit string of random alphanumeric characters that can only be unlocked with a **key** by the **receiver** . SET adds a digital signature to SSL for unassailable proof that the bearer of a credit-card number is authentic. SET can help merchants avoid current money-losing scenarios in which people say they did not order an item or service on a particular credit card number that was given to a merchant.

REVISION DATE: 20030428

25/7/12
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00100885 DOCUMENT TYPE: Review

PRODUCT NAMES: Pretty Good Privacy for Mail 4.5 (647039)

TITLE: PGP Gets Click-Simple
AUTHOR: Kantor, Andrew
SOURCE: Internet World, v8 n4 p26(1) Apr 1997
ISSN: 1097-8291
HOMEPAGE: http://www.iw.com

RECORD TYPE: Review
REVIEW TYPE: Review
GRADE: A

Pretty Good Privacy for Mail (PGPMail) 4.5 from Pretty Good Privacy improves on an already strong e-mail encryption and digital signing program. With PGP (Pretty Good Privacy) 4.5, the process of encryption and/or digitally signing an e-mail message is simplified so that it will appeal to a wider audience. With PGPmail 4.5, encryption and digital signing are integrated in the toolbar of the e-mail applications of Qualcomm's Eudora and Netscape's Mail. PGP is working on plug-ins for other applications, in an effort to set up PGP as the product that will push e-mail encryption and signatures into the mainstream. Encryption is a method of ensuring that e-mail messages can only be read by the person intended to read them. PGP uses a new method of working with a key, or secret code, called public-key (or asymmetric) encryption. Users possessing someone's public **key** can **send** a message that only that person can see, using the secret key. Formerly, PGP **encrypted** **messages** went through steps involving different files. With this new streamlined and more secure version, PGP makes it easy to send secure, private messages.

REVISION DATE: 20020321

25/7/13
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00098558 DOCUMENT TYPE: Review

PRODUCT NAMES: Pretty Good Privacy for Mail (647039)

TITLE: PGP tool adds key to secure intranet **mail**
AUTHOR: Jones, Chris
SOURCE: InfoWorld, v18 n49 p1(2) Dec 2, 1996

ISSN: 0199-6649
HOMEPAGE: http://www.infoworld.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

Pretty Good Privacy's (PGP's) Pretty Good Privacy for Mail, a 128-bit e-mail encryption application used by about 2 million users as freeware, will be released commercially early in 1997 with a new graphical user interface (GUI). The new release of PGP for Mail will allow users to embed digital signatures, compress **data** before **encryption** , and manage public keys. Public keys allow distribution of **encrypted messages** with digital signatures that recognize the sender. The tool will help ensure more secure **intranets** , and end-users can also use the mail encryption to protect their privacy. An analyst says employees' rights have to be addressed as businesses implement encrypted e-mail, so that workable policies can be designed and used. Phil Zimmerman, chairman of PGP, says his company intends to protect the privacy of individual missives and corporate assets. For instance, certified corporate key displays will permit security officers to control the use of public and private keys, including which ones are used, where **encrypted messages** may be sent, and methods of **data encryption** . Zimmerman says workers should have control over their own e-mail keys, but that corporations should control keys for corporate assets. With public key encryption, individual private **key** holders can **send encrypted messages** with digital signatures, and the signatures can be validated with a public key made 'available to anyone and then later decrypted using the recipient's private key.'

REVISION DATE: 20020321

25/7/14

00095905 DOCUMENT TYPE: Review

PRODUCT NAMES: Company--Cisco Systems Inc (850187)

TITLE: The Rules According To Cisco
AUTHOR: Janah, Monua
SOURCE: Information Week, v597 p18(3) Sep 16, 1996
ISSN: 8750-6874
HOMEPAGE: http://www.informationweek.com

RECORD TYPE: Review
REVIEW TYPE: Company

Cisco Systems, once known only for its **networking** routers, has in the last three years acquired companies and products that vaulted it into every corner of the **inter**networking hardware business. Cisco is also bent on making its foundational **network** operating system (NOS) an industry standard for **networking** , with support for **Internet** appliances, central office switches, and every box in between. John Chambers, president and CEO, says, 'We went for market share in each segment, and now we are tying the products in each segment together with software.' Cisco is integrating its **Internetworking** Operating System (IOS) with the BPX wide area switch acquired with StrataCom, and will enhance the IOS to support burgeoning **Internet / intranet** markets. New features include **encryption** for bulk

data transfers ; **key** management for secure sessions; Domain Name System certificates; and enhanced **virtual** private **network** functions, including secure dial-up. Cisco's strategy is discussed in some detail.

REVISION DATE: 20020703

25/7/15
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00093089 DOCUMENT TYPE: Review

PRODUCT NAMES: Encryption (832022)

TITLE: Data Security: key issue **in an age of pervasive computing**
AUTHOR: Strassberg, Dan
SOURCE: EDN Magazine, v41 n8 p48(7) Apr 11, 1996
ISSN: 0012-7515
HOMEPAGE: http://www.ednmag.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

Philip Zimmermann's Pretty Good Privacy, DSS, and IBM's DES are part of a discussion of data security measures, which can be implemented using a combination of techniques. One good security measure is National Semiconductor's PersonalCard data-security PCMCIA cards, which are portable individual 'tokens' that control access to wired and wireless **networks** and **network** resources, including databases. The cards **encrypt** /decrypt **data** , so that private information can be protected from authorized **network** users not cleared to view the data. Threats to national security are as severe from inside the U.S. as from outside, which has prompted the government to develop key-escrow methods like Clipper that allow the federal government access to **encrypted data** sent inside the U.S. Other topics discussed include manufacturers of data security products; asymmetry; secret-key systems; and one-way hash functions.

REVISION DATE: 20000730

25/7/16
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00091489 DOCUMENT TYPE: Review

PRODUCT NAMES: Entrust Lite Windows (617652)

TITLE: Don't Lose Your Crypto Keys
AUTHOR: Wayner, Peter
SOURCE: Byte, v21 n5 p137(1) May 1996
ISSN: 0360-5280
HOMEPAGE: http://www.byte.com

RECORD TYPE: Review
REVIEW TYPE: Review
GRADE: A

Nortel's Entrust Life for Windows is a basic but competent key management product that provides a way to encrypt e-mail throughout the enterprise. Entrust Manager maintains a user-friendly list of private and public key pairs. Entrust Client **encrypts** , decrypts, or signs **files** using either DES or Nortel's CAST algorithm. Public key encryption is based on the Rivest-Shamir-Adleman algorithm. Encryption is with a session key that is encrypted with the public **key** of each authorized **receiver** . Therefore, the file can be stored in a public directory and access permitted for any number of users. Entrust works with Microsoft Mail and cc:Mail, although automation features would make encryption less task intensive. Entrust, which must be activated by the user or by a custom-written program, is recommended as one of the most comprehensive encryption and key maintenance systems available.

REVISION DATE: 20010830

25/7/17
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00091195 DOCUMENT TYPE: Review

PRODUCT NAMES: SafE Mail 1.12 (614327)

TITLE: SafE Mail 1.12 provides secure correspondence in Windows
AUTHOR: Senna, Jeff
SOURCE: InfoWorld, v18 n22 pN/2(1) May 27, 1996
ISSN: 0199-6649
HOMEPAGE: http://www.infoworld.com

RECORD TYPE: Review
REVIEW TYPE: Review
GRADE: A

SafE Mail's 1.12 e-mail encryption product protects documents from unauthorized access. It converts files to an ASCII text **Internet** -compatible format using proprietary encryption/decryption. A public-key/private-key protocol combo is used at installation so users can make documents secure from the desktop. During tests, a public **key** was **sent** to another user, who **encrypted** a **message** using the public key. The message was then decrypted by the recipient with the private key. This method requires SafE Mail installation and configuration on each machine. Encryption is to a text file, which is launched as an attachment in an e-mail program. SafE Mail operation is smooth, and the software can be installed locally or on a **network** drive. The user personalizes the disk with public and private keys, to allow encryption/decryption on another machine such as a laptop.

REVISION DATE: 20000630

25/7/18
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00088502 DOCUMENT TYPE: Review

PRODUCT NAMES: NetLOCK (487899)

TITLE: NetLock secures net transactions
AUTHOR: Pearlstein, Joanna
SOURCE: MacWEEK, v10 n5 p14(2) Feb 5, 1996
ISSN: 0892-8118
HOMEPAGE: http://www.macweek.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

Hughes Aircraft has announced a **client / server** package for **encrypting packets** over **LANs** and **WANs** . Its NetLOCK software establishes a cryptographic envelope that protects data sent over both public and private **networks** . It creates a unique encryption **key** for each **transmission** and an automatic peer-to-peer encryption and authentication session. There are two parts to the software, the NetLOCK manager and an extension that is installed on client systems. The management application resides on a server, and the client software is transparent to end-users. Manager allows administrators to select from multiple encryption algorithms.

REVISION DATE: 20020630

25/7/19
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00086862 DOCUMENT TYPE: Review

PRODUCT NAMES: Encryption (832022)

TITLE: Packet encryption **may bury security concerns**
AUTHOR: Bird, Patrick
SOURCE: Network World, v12 n48 p45(1) Nov 27, 1995
ISSN: 0887-7661
HOMEPAGE: http://www.nwfusion.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

Packet encryption technology, often implemented on Asynchronous Transfer Mode (ATM) and frame relay services-based systems, could replace current transaction security methods. **Packet encryption encrypts** a transmission at the **network** layer of the Open Systems Interconnection model, including the IP header. A new, readable header is provided that is the IP address of the destination site. The complete encrypted transaction moves across a router-based IP **network** without modification. Transmissions are sent over multiple **virtual** circuits on a **WAN** without sacrificing security. **Packet encryption** can also apply keys flexibly to data traffic. For example, an encryption device could be coded to apply a stipulated **encryption key** to **data sent** from one IP **subnet** to another. With **packet encryption** , **network** managers can more easily deploy redundant machines to protect from single-point-of-failure breakdowns.

REVISION DATE: 20020630

25/7/20

DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.
(c)2003 Info.Sources Inc. All rts. reserv.

00084372 DOCUMENT TYPE: Review

PRODUCT NAMES: Encryption (832022)

TITLE: Encryption: Keeping the network **safe from prying eyes**
AUTHOR: Shannon, Sherry E
SOURCE: Computing Canada, v21 n19 ps11(1) Sep 13, 1995
ISSN: 0319-0161
HOMEPAGE: http://www.plesman.com/cc

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

Decentralized computing systems, including those used in concurrent design, need data security and integrity and cryptographic systems provide it. Symmetric key and public key systems are used. Symmetric key systems use an identical key for both encryption and decryption. Therefore, only the sender and **receiver** can know the **key** if the system is to be truly secured. Public key systems use two different keys, a public key and a private key, to encrypt and decrypt. The keys are mathematically associated, but private key information cannot be processed on a computer to detect the public key. Public key systems also have separate encryption and decryption stages, allowing **messages** to be **encrypted** so that only one person can read them. The Elliptic Curve Cryptosystem is a public key system that provides the advantages of high speed, low power requirements, and a smaller key size.

REVISION DATE: 20020630

25/7/21
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.
(c)2003 Info.Sources Inc. All rts. reserv.

00083063 DOCUMENT TYPE: Review

PRODUCT NAMES: SSL (835111)

TITLE: Internet **Commerce and Security**
AUTHOR: Marks, Daniel
SOURCE: Chicago Computer Guide, v10 n7 p22(1) Jul 1995
ISSN: 1071-7749
HOMEPAGE: http://www.Chicago-Computer.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

The **Internet** is quickly becoming like the suburbs, with a number of shops popping up all over the place. Of course as more business takes place on the **Internet** , it leaves people more vulnerable to fraud. The primary protection against **Internet** fraud is cryptography: **ciphering** a **message** so only the people who are supposed to see the message can see it. Cryptography has advanced so that now even the **key** can be **sent** through the **Internet** safely. There is a push for encrypting the World Wide **Web** , since a great deal of business takes place there. SSL is one program that

can be used for protection anywhere in the **Internet** , but it only supports RSA public-key encryption.

REVISION DATE: 20010330

25/7/22
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.
(c)2003 Info.Sources Inc. All rts. reserv.

00082950 DOCUMENT TYPE: Review

PRODUCT NAMES: Encryption (832022)

TITLE: Encryption Addresses Privacy, Authentication and Data Integrity
AUTHOR: Bowen, Barry D
SOURCE: Client/Server Computing, v2 n10 p50(6) Oct 1995
ISSN: 1059-3470

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

Most major businesses want encrypted security tools to ensure privacy of messages, and integrity of transactions. The availability of public key encryption techniques makes encryption much simpler. This technique provides an easy way to securely provide a recipient with a key to unscramble data. This technology is often used for digital signatures, for **encrypting messages** , and for initiating **encrypted** sessions that will be used with private key encryption methods. Private key uses the same key to **encrypt** and decrypt **data** . Public key **encryption** , on the other hand, uses four **keys** . Both **sender** and recipient hold a unique public and private key, with the public keys being freely distributed. Dedicated encryption devices, sometimes added in to firewall devices, are often necessary to maximize a sustained data throughput.

REVISION DATE: 20020630

25/7/23
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.
(c)2003 Info.Sources Inc. All rts. reserv.

00079848 DOCUMENT TYPE: Review

PRODUCT NAMES: SecurPC (546232)

TITLE: RSA: Software's Sign Of Security
AUTHOR: Steinert-Threlkeld, Tom
SOURCE: Interactive Week, v2 n12 p41(2) Jun 19, 1995
ISSN: 1078-7259
HOMEPAGE: http://www.interactive-week.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

RSA Data Security hopes to make its double-key logo a standard which software vendors will place on their boxes as a sign of security. RSA's encryption schemes will work on millions of PCs without end users even

realizing it. Lotus Notes uses RSA security, and RSA technology is rapidly becoming the standard for secure transactions on the World Wide Web. Two potential data security standards, Secure HTTP and Secure Sockets Layer, are both based on RSA technology. RSA security technology is built around the concept of a dual-key system, where one key is made available publicly, and the other is kept private. The approach is better than a solely private key system, since as private keys continue to get distributed, it is likely that they will fall into the wrong hands. The dual- **key** system lets a **sender** **encode** a **message** with a public key, but only the intended recipient can decode it with the private key. The digital signature concept also verifies the precise source of the message.

REVISION DATE: 20010930

25/7/24
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00076691 DOCUMENT TYPE: Review

PRODUCT NAMES: Pretty Good Privacy (835072)

TITLE: World's Easiest Fake I.D.
AUTHOR: Richardson, Robert
SOURCE: LAN Magazine, v10 n4 p29(1) Apr 1995
ISSN: 1069-5621

RECORD TYPE: Review
REVIEW TYPE: Review
GRADE: A

Users can download the Pretty Good Privacy freeware encryption program from the **Internet** or purchase it from ViaCrypt. The program gives users a way to force credential authentication; in this way, those doing business on the **Internet** can determine if a correspondent is a straight-arrow merchant or a potential thief. PGP provides two personal keys--a public key and a private key--generated by the user. The two are matched, and one is used to show **data** **encrypted** by the other. If a user sends an **encrypted** **message** , the **file** is **encrypted** using the **receiver** 's public **key** . When the message is received, the recipient processes it through the private key to decrypt. According to the developer of PGP, the validity of user-defined public keys is equivalent to that of today's handwritten signatures, and offers better security than central authority-maintained public keys.

REVISION DATE: 20010330

25/7/25
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00070327 DOCUMENT TYPE: Review

PRODUCT NAMES: Pretty Good Privacy (835072)

TITLE: A Privacy Advocate Draws the Blinds on Big Brother
AUTHOR: Dewar, Robert B K Smosna, Matthew
SOURCE: Open Systems Today, v162 p56(3) Oct 31, 1994

ISSN: 1061-0839

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

Phil Zimmerman's PGP (Pretty Good Privacy) public-key encryption package is freely available on the **Internet** for private and noncommercial use, and is available on a variety of platforms. PGP is in the middle of a controversy involving the National Security Agency. The NSA has had a monopoly on cryptographic techniques until the release of PGP. A public key system uses two encryption keys, one public and one private, for the secure exchange of **messages** . **Encrypted messages** are **sent** with the public **key** , and decoded with the private key. PGP is based on the RSA algorithm, which factors large numbers into their prime-number components. The algorithm can also attach digital signatures to secret messages.

REVISION DATE: 20010330

25/7/26
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00069595 DOCUMENT TYPE: Review

PRODUCT NAMES: Internet **Security (841944**

TITLE: Internet **Security Gets Boost**
AUTHOR: Rodriguez, Karen
SOURCE: InfoWorld, v16 n40 p1(2) Oct 3, 1994
ISSN: 0199-6649
HOMEPAGE: http://www.infoworld.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

Internet users will soon benefit from Secure HTTP technology, which enables **data encryption** , authentication, and digital signatures. These are functions usually found in dedicated line connections. The technology, developed by Enterprise Integration Technologies Corporation, a research and development firm, uses public **key** encryption and Hypertext **Transfer** Protocol. HTTP is the transmission protocol used by the World Wide **Web** on the **Internet** . Secure HTTP's foundation is encryption certified for overseas use, and also works with other cryptography products. The product includes Domain Security Administration algorithms. The complete function set allows businesses to authenticate trading partner identity. According to an executive banker interviewed, Secure HTTP provides enabling technology that extends banking to the **Internet** .

REVISION DATE: 20010330

25/7/27
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00068714 DOCUMENT TYPE: Review

PRODUCT NAMES: Computer Security (830071)

TITLE: Database Security in a Client / Server **World**
AUTHOR: Bobrowski, Steve
SOURCE: DBMS, v7 n10 p48(5) Sep 1994
ISSN: 1041-5173
HOMEPAGE: http://www.dbmsmag.com

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

Client / server computing brings many advantages, although establishing security on the **network** is often a problem. The **network** that connects the **clients** with the **servers** is inherently insecure, and can be easily broken into with publicly available utilities. Other programs are readily available that will allow an attacker to sniff the **network** to read information packets. The first defense is user identification and authentication. Good password security is essential, and users should avoid using short or easily guessed passwords. Security is also essential at the database level. Encryption can solve many of the security problems. Secret-key encryption is commonly used, but requires careful key management. Public-key encryption solves some **key** management **issues** , since messages are **sent** via a public **key** cryptosystem, but decoded upon receipt with a separate, private key.

REVISION DATE: 20020630

25/7/28
DIALOG(R)File 256:SoftBase:Reviews,Companies&Prods.

00065453 DOCUMENT TYPE: Review

PRODUCT NAMES: SecureWeb (543392); Mosaic for CommerceNet (515655)

TITLE: Two Companies Team Up to Tackle A Key Problem
AUTHOR: Wagner, Mitch
SOURCE: Open Systems Today, v152 p1(2) Jun 20, 1994
ISSN: 1061-0839

RECORD TYPE: Review
REVIEW TYPE: Product Analysis
GRADE: Product Analysis, No Rating

SecureWeb and Mosaic for CommerceNet are tools that allow users to write secure **Internet** applications. Users can exchange confidential data, including credit card numbers and proprietary corporate information via applications that operate on the World Wide **Web** , according to a principal involved. SecureWeb uses technology known as public **key** encryption. Users can **send encrypted data** , and the software validates messages to remove the possibility of forgery or modification during transmission. Two companies developing the technology placed a specification for Secure HyperText Transaction Protocol (S-HTTP) into the public domain recently; it can be obtained on the **Web** or via anonymous ftp. **Client** and **server** versions of HTTP are available, and Mac, Microsoft Windows, and UNIX OSs will be supported.

REVISION DATE: 20010730

```
File   9:Business & Industry(R) Jul/1994-2003/Jul 30
         (c) 2003 Resp. DB Svcs.
File  16:Gale Group PROMT(R) 1990-2003/Jul 31
         (c) 2003 The Gale Group
File  47:Gale Group Magazine DB(TM) 1959-2003/Jul 23
         (c) 2003 The Gale group
File 148:Gale Group Trade & Industry DB 1976-2003/Jul 31
         (c)2003 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
         (c) 1999 The Gale Group
File 275:Gale Group Computer DB(TM) 1983-2003/Jul 31
         (c) 2003 The Gale Group
File 621:Gale Group New Prod.Annou.(R) 1985-2003/Jul 31
         (c) 2003 The Gale Group
File 636:Gale Group Newsletter DB(TM) 1987-2003/Jul 31
         (c) 2003 The Gale Group
? ds

Set     Items   Description
S1    3150984   KEY? ? OR CIPHER? OR CYPHER? OR ALGORITHM?
S2     144475   S1(3N)(SEND??? ? OR SENT OR TRANSMIT? OR TRANSMIS? OR TRAN-
              SFER? OR XFER? OR DELIVER? OR ISSUE? ? OR ISSUING OR ISSUANCE?
               OR RECEIV? OR RECEIPT? ? OR RECEPTION?)
S3     415303   CIPHER? OR CYPHER? OR ENCIPHER? OR ENCYPHER? OR ENCRYPT? OR
              SCRAMBL? OR ENCOD???? ?
S4      97416   S3(3N)(DATA OR INFORMATION OR PACKET? ? OR MESSAG??? ? OR -
              FILE OR FILES OR CONTENT)
S5       8327   S4(3N)(USER? OR CLIENT? OR RECIPIENT? OR BUYER? OR RECEIVE-
              R? OR PATRON? OR PURCHASER? OR CONSUMER? OR CUSTOMER? OR SHOP-
              PER? OR SUBSCRIBER?)
S6        145   S4(3N)(REQUEST?R? ? OR ESHOPPER? OR PARTICIPANT? OR MEMBER?
               ? OR NETIZEN?)
S7        845   S4(3N)(INDIVIDUAL? ? OR PERSON? ? OR PARTY)
S8       6948   S2(3N)(USER? ? OR CLIENT? OR RECIPIENT? OR BUYER? OR PATRO-
              N? OR PURCHASER? OR CONSUMER? OR CUSTOMER? OR SHOPPER? OR SUB-
              SCRIBER?)
S9       1781   S2(3N)(REQUEST?R? ? OR ESHOPPER? OR PARTICIPANT? OR MEMBER?
               ? OR NETIZEN? OR INDIVIDUAL? ? OR PERSON? ? OR PARTY)
S10       404   S2(S)S5:S7
S11       122   S10(S)S8:S9
S12       436   S9:S10(S)S4
S13      2771   UNENCRYPT? OR UNENCIPHER? OR UNENCYPHER? OR UNCRYPT? OR UN-
              CYPHER? OR UNCIPHER? OR NONCRYPT? OR NONCIPHER? OR NONCYPHER?
              OR NONSCRAMBL?
S14       111   NONENCRYPT? OR NONENCIPHER? OR NONENCYPHER?
S15       474   (NON OR UN)()(ENCRYPT? OR ENCIPHER? OR ENCYPHER? OR CRYPT?
              OR CYPHER? OR CIPHER? OR ENCOD????)
S16       314   NONENCOD? OR UNENCOD?
S17      3811   (S3 OR S13:S16)(3N)(PARTIAL? OR PARTLY OR PART OR PARTS OR
              PORTION? OR SECTION? ? OR SEGMENT? ?)
S18         3   S12(S)S17
S19         0   S10(S)S17
S20        49   S17(S)S2
S21        74   S17(S)S5:S7
S22        14   S8:S9(S)S17
S23       123   S18:S22
S24        37   S23/2000:2003
S25        86   S23 NOT S24
S26        52   RD (unique items)
S27        23   S11/2000:2002
S28        95   S11 NOT (S27 OR S23)
```

S29 61 RD (unique items)
? t29/3,k/2,5-6,10,12,15

29/3,K/2 (Item 2 from file: 9)
DIALOG(R)File 9:Business & Industry(R)
(c) 2003 Resp. DB Svcs. All rts. reserv.

2139330 Supplier Number: 02139330 (USE FORMAT 7 OR 9 FOR FULLTEXT)
Banks rush to become CAs
(UK and US financial institutions seek to become digital certification authorities in bid to capture profits from expected growth in electronic commerce revenues to $6.8 bil in 2000, vs $800 mil in 1997)
Electronic Payments International, n 130, p 9
May 1998
DOCUMENT TYPE: Newsletter ISSN: 0954-0393 (Ireland)
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 1416

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:
...Encryption of Internet-based data is normally carried out using a dual-key system. Each **party** holds a public **key** , which is **sent** with any **encrypted data** to the **recipient** , and a private key, which is combined with the public **key sent** by the dispatcher to provide the means to decrypt the information on receipt.

To guarantee...

29/3,K/5 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2003 The Gale Group. All rts. reserv.

07059715 Supplier Number: 59271263 (USE FORMAT 7 FOR FULLTEXT)
Raze Your RAS.(Technology Information)
ROSEN, MICHELE
ENT, v2, n15, p52
Oct 8, 1997
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Professional
Word Count: 663

... connects to the Internet using the local Internet service provider, and then activates the tunneling **client** , which **sends** the necessary **keys** to authenticate itself and the server. The software then inserts itself into the IP protocol stack, so that all packets transmitted from the **client** are **encrypted** , and all **packets** received are decrypted. This eliminates the need for application-specific encryption, Suarez notes. "All applications...

29/3,K/6 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2003 The Gale Group. All rts. reserv.

06578110 Supplier Number: 55512537 (USE FORMAT 7 FOR FULLTEXT)
The Sources Of Production.(data warehousing)(Technology Information)
HP Professional, v13, n8, p46
August, 1999

Language: English Record Type: Fulltext Abstract
Document Type: Magazine/Journal; Trade
Word Count: 1298

... data warehousing community and is generating eminently workable solutions.

Many data warehouses require that all **usernames** , passwords and returned information be **encrypted** . **Users** **receive** a public **key** **issued** by a certificate authority and stored on the Web browser. A private key at the...

29/3,K/10 (Item 6 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2003 The Gale Group. All rts. reserv.

05966683 Supplier Number: 53250334 (USE FORMAT 7 FOR FULLTEXT)
Digital certificates are the key behind electronic commerce.(public key encryption systems)(Technology Information)
Computer Weekly, p36(1)
Nov 12, 1998
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 428

... problems arise when your public key is intercepted and replaced by the interceptor's public **key** which is then **sent** onto the **recipient** . If the recipient subsequently used this public key to **encrypt** **data** , the **person** who did the intercepting would be in a position to decrypt it with his or...

29/3,K/12 (Item 8 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2003 The Gale Group. All rts. reserv.

05751122 Supplier Number: 50234601 (USE FORMAT 7 FOR FULLTEXT)
Making E-Mail Secure: Here's how S/MIME can safeguard your communication--and why it sometimes doesn't
Canter, Sheryl
PC Magazine, v17, n15, p263
Sept, 1998
Language: English Record Type: Fulltext
Article Type: Article
Document Type: Magazine/Journal; General Trade
Word Count: 3364

... of PC Magazine.

Figure 1: When user A wants to send a secure message to **user** B, he encrypts the **message** with **user** B's public **key** . When **user** B **receives** the message, he decrypts it with his private key.

29/3,K/15 (Item 11 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2003 The Gale Group. All rts. reserv.

04992163 Supplier Number: 47332413 (USE FORMAT 7 FOR FULLTEXT)
Data security chips ward off intrusions
Takahashi, Richard

Electronic Engineering Times, p098
April 28, 1997
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1747

... algorithms to commercial use. Public-key algorithms do not rely on the same key to **encrypt** and decrypt operations. Message transmitter and **receiver** hold different **keys** . To **send** a message, the transmitter and **receiver** exchange their **keys** . The message **transmitter** combines his or her key with the **recipient** 's private **key** and **sends** the message. Public- **key** algorithms do not require both keys to be secret or private. Only one of the...
? t29/3,k/35

29/3,K/35 (Item 4 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

11538825 SUPPLIER NUMBER: 57749097 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Reel to real: should you believe what you see?(computer-generated evidence)
Harts, Dean M.
Defense Counsel Journal, 66, 4, 514
Oct, 1999
ISSN: 0895-0016 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 7116 LINE COUNT: 00583

... or encrypt the data file; the second is used to verify the signature or de- **encrypt** the **data file** .
Each **party** using digital signatures has a "public key" and a "private key." The public key is openly distributed; the private key is kept confidential. The **person** who **encrypts** a digital **message** uses the **recipient** 's public **key** and **sends** the message. Now, only the recipient's private key can decipher the message, and anyone...

...the message cannot read it. Thus, the sender and recipient need not share any confidential **key** , and each can **send** and receive secure digital messages.(65)
B. Use Hash Marks
Another option involves running a...
? t29/3,k/40,46,49

29/3,K/40 (Item 9 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB

08121248 SUPPLIER NUMBER: 17380463 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Doing business on the Internet - a question of balance. (includes related article)
Arnum, Eric
Business Communications Review, v25, n8, p35(3)
August, 1995
ISSN: 0162-3885 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 2696 LINE COUNT: 00214

... the listed sender and that it is unchanged from the original.
* Privacy: A sender can **encrypt** a **message** with the **recipient** 's public key, which can be obtained from an agreed on source such as a common directory, a key management system or even the **recipient** . Only the **receiver** 's private **key** can decrypt the message, and there might also be

a digital signature within the envelope...

29/3,K/46 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2003 The Gale Group. All rts. reserv.

02166613 SUPPLIER NUMBER: 20085999 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Strictly confidential. (five encryption software packages reviewed) (Software Review) (Evaluation)
Haskin, David
Computer Shopper, v18, n1, p344(3)
Jan, 1998
DOCUMENT TYPE: Evaluation ISSN: 0886-0556 LANGUAGE: English
RECORD TYPE: Fulltext; Abstract
WORD COUNT: 2471 LINE COUNT: 00205

... keys are less secure than private keys, but in this case, both are required to **encrypt** and decrypt **data** . You **encrypt** information using the **recipient** 's public **key** . The **recipient** can **send** you this public **key** via nonsecure methods such as e-mail, or it can be stored in a network ...

29/3,K/49 (Item 4 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2003 The Gale Group. All rts. reserv.

01915555 SUPPLIER NUMBER: 18109672 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Nortel, HP keep Open Mail closed. (integrating security technology into HP OpenMail E-mail system) (Brief Article) (Product Announcement)
LAN Magazine, v11, n4, p24(1)
April, 1996
DOCUMENT TYPE: Brief Article Product Announcement ISSN: 1069-5621
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 339 LINE COUNT: 00029

... matching public key. The public keys are given out to other users, who employ a **user** 's public **key** to **send** that **person** an **encrypted message** . The only key that can decrypt the message is the recipient's private key. People...
? t29/3,k/53

29/3,K/53 (Item 8 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2003 The Gale Group. All rts. reserv.

01690848 SUPPLIER NUMBER: 15562797 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Confidentially speaking. (E-mail security) (Cover Story)
Stallings, William
LAN Magazine, v9, n8, p49(4)
August, 1994
DOCUMENT TYPE: Cover Story ISSN: 0898-0012 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 3186 LINE COUNT: 00252

... first scenario, the sender can encrypt with his or her private key, and then the **recipient** decrypts with the **sender** 's corresponding public **key** . In the second scenario, the sender can encrypt with the recipient's public key, and...

...the recipient decrypts with the recipient's corresponding private key. In this way, anyone can **encrypt** a block of **data** using a **recipient** 's public key, and only the intended recipient will be able to decrypt the block...
?

26/3,K/1 (Item 1 from file: 9)
DIALOG(R)File 9:Business & Industry(R)

1586830 Supplier Number: 01586830 (USE FORMAT 7 OR 9 FOR FULLTEXT)
TECHNOLOGY: Any time, anywhere Many banks want to hook up to the Internet but are concerned about security, says George Cole:
(About 50m people have access to the Internet but this number is expected to reach 200m within two years; banks look to this market)
Financial Times London Edition, p 20
September 05, 1996
DOCUMENT TYPE: Business Newspaper; Industry Overview ISSN: 0307-1766 (United Kingdom)
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 1202

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:
...the customer authorised a particular transaction."

A digital signature is created by the sender, who **encrypts part** of the message with his or her private key. The recipient of the message uses the **sender** 's public **key** to decrypt the segment and thus confirm the identity of the sender. The system will...

26/3,K/2 (Item 2 from file: 9)
DIALOG(R)File 9:Business & Industry(R)

1333101 Supplier Number: 01333101 (USE FORMAT 7 OR 9 FOR FULLTEXT)
Sun Pushes for Wider Acceptance of SKIP
(Sun Microsystems pushing its SKIP technology as standard for Internet Protocol-based security in the corporate enterprise)
CommunicationsWeek, n 584, p 5
November 13, 1995
DOCUMENT TYPE: Journal ISSN: 0748-8121 (United States)
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 402

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:
...Photuris, which directly competes with SKIP for security standards.

SKIP and Photuris both address the **issue** of **key** management, a vital **part** of the **encryption** process that creates, distributes and authenticates public and private keys between communicating parties. Without this...

26/3,K/3 (Item 3 from file: 9)
DIALOG(R)File 9:Business & Industry(R)

1121585 Supplier Number: 01121585 (USE FORMAT 7 OR 9 FOR FULLTEXT)
Europeans combat car thefts with immobilizer

(In 1993, 13 of every 1,000 vehicles in France were stolen, vs 8 of every 1,000 in US; notes Ford's Passive Anti-Theft System)
Automotive News, n 5590, p 20
February 06, 1995
DOCUMENT TYPE: Journal ISSN: 0005-1551 (United States)
LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 328

(USE FORMAT 7 OR 9 FOR FULLTEXT)

TEXT:
...if they wanted full insurance reimbursement on a stolen car.

An immobilizer has two main **parts** : a tiny **encoded transmitted** embedded in a **key** and a **receiver** encircling the ignition.

When the driver inserts the key in the ignition, the receiver picks...

26/3,K/4 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2003 The Gale Group. All rts. reserv.

06866066 Supplier Number: 58180915 (USE FORMAT 7 FOR FULLTEXT)
Self-destructing e-mail: pragmatic or paranoid?(Disappearing Inc.'s e-mail technology) (Above the Clouds)(Company Business and Marketing)(Column)
Kobielus, James
Network World, p53
Nov 29, 1999
Language: English Record Type: Fulltext
Article Type: Column
Document Type: Tabloid; Trade
Word Count: 731

... those messages have been received, read and archived. The company manages this trick by enabling **users** to **encrypt message** body **parts** and then require recipients to retrieve centrally stored, message-specific decryption keys every time they...

26/3,K/5 (Item 2 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2003 The Gale Group. All rts. reserv.

06081939 Supplier Number: 53592919 (USE FORMAT 7 FOR FULLTEXT)
Digital Certificates Take Hold in Ontario.(Company Business and Marketing)
Ploskina, Brian
ENT, v4, n2, p32(1)
Jan 20, 1999
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Professional
Word Count: 551

... PKI is basically a two-part system. The first part is distributive: certificate holders deliver **part** of their **encryption** key to people or agencies that may want to reach them. High-level PKIs scramble...

...1,024 bits. It is virtually impossible to crack without the second half of the **key** . Once data is **sent** , the privately held second half of the PKI is used to decode it.

This technology...

26/3,K/6 (Item 3 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

05912254 Supplier Number: 53137284 (USE FORMAT 7 FOR FULLTEXT)
Security you can bank on.(Industry Trend or Event)
Communications News, p26
Oct 1, 1998
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 1449

... system and proceeds with the work at hand. No specific activity on the user's **part** is required to **encrypt** queries or commands, or to decrypt responses. The outgoing message is loaded automatically into the...

...is sent to the LVTS mainframe. At no point does the digital signature or encryption **key** leave the token.
SENT TO MAINFRAME
The message is sent over a commercial frame-relay circuit to the LVTS
...

26/3,K/7 (Item 4 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

05736126 Supplier Number: 50215610 (USE FORMAT 7 FOR FULLTEXT)
IPSec-Compliant VPN Solutions: Virtualizing Your Network
Fratto, Mike
Network Computing, p72
August 1, 1998
Language: English Record Type: Fulltext
Article Type: Article
Document Type: Magazine/Journal; Trade
Word Count: 3788

... since keys can't be updated as often.
You also need a secure way to **transmit** those **keys** to other devices. IKE automates the process by using public-key cryptography to create a...

...such as rekeying the VPN while in session (if one key is compromised, only the **portion** **encrypted** with that key is recoverable) and perfect forward secrecy (no two keys are related).
At...

26/3,K/8 (Item 5 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

05393890 Supplier Number: 50296546 (USE FORMAT 7 FOR FULLTEXT)
SECURITY CORDONS
Harrington, Tony
Unix & NT News, p42
Oct, 1997

Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 2227

... Alternatively, the more sophisticated firewalls could become access routers,' he says.
Mere technology aside, the **encryption part** of the security equation is a particularly hot political topic at the moment. Civil liberties...

...on the likes of criminals, terrorists and drug smugglers. Accordingly, they want companies and private **individuals** using **data encryption** to be forced to deposit decrypting keys with some trusted third party. This is not...

26/3,K/9 (Item 6 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2003 The Gale Group. All rts. reserv.

05233927 Supplier Number: 47980902 (USE FORMAT 7 FOR FULLTEXT)
RecoverKey Unlocks Data
Phillips, Ken
PC Week, v14, n39, p138
Sept 15, 1997
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Tabloid; General Trade
Word Count: 1321

... time that it becomes impractical to use this system to encrypt long messages.
As a **partial** solution, most current **encryption** products use a combination of both symmetric and asymmetric methods. A DES (symmetric) session key...

...used to encrypt the message, while the session key is encrypted using the public/private **key** method and **sent** along with the message in the header.
The recipient can use the key he or...

26/3,K/10 (Item 7 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2003 The Gale Group. All rts. reserv.

05148060 Supplier Number: 47857915 (USE FORMAT 7 FOR FULLTEXT)
TIS Ships "Total Solution" For User Controlled Encryption Key Recovery.
Business Wire, p7251232
July 25, 1997
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 990

... engine to generate a "key recovery field" for a message or file as an integral **part** of the **encryption** process. The hidden "spare key" stays securely locked up in its key recovery field and...

...center. Users maintain control of their keys and their files. If recovery is needed, the **key** recovery center is **sent** only the **key** recovery field, not the encrypted data. Already licensed by IBM (NYSE:

IBM), Atalla Corporation (A...

26/3,K/11 (Item 8 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

04878785 Supplier Number: 47177232 (USE FORMAT 7 FOR FULLTEXT)
Congress Vs. President On Encryption
Kapustka, Paul
CommunicationsWeek, p1
March 3, 1997
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 770

... bone of contention is the administration's desire to make key recovery and escrow technology **part** of all exportable **encryption** products. Encryption "keys" allow **users** to **scramble** and unscramble **data** or communications. The administration claims that without easy access to keys, criminals would be able...

26/3,K/12 (Item 9 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

04528971 Supplier Number: 46654196 (USE FORMAT 7 FOR FULLTEXT)
Buying data bit by bit with microcash; New technology lets Internet users pay as they go
PC Week, pN03
August 26, 1996
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Tabloid; General Trade
Word Count: 1671

... steps of the transaction than Millicent's server.
In negotiations
In a novel approach, NetBill **encrypts** the goods sent, **partly** to ensure that delivery is acknowledged. Once the price has been negotiated between the customer...

...the customer is legitimate (for example, not using stolen tokens), only then will the merchant **send** a **key** to the **customer** for decrypting the purchased item.
This "certified delivery," as NetBill's developers call it, should...

26/3,K/13 (Item 10 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

04427465 Supplier Number: 46495777 (USE FORMAT 7 FOR FULLTEXT)
VISA, MASTERCARD AND TECHNOLOGY PARTNERS PUBLISH REVISED SECURE ELECTRONIC TRANSACTIONS METHOD
PR Newswire, p626LAW025
June 26, 1996
Language: English Record Type: Fulltext
Document Type: Newswire; Trade
Word Count: 592

... GTE, IBM, Microsoft, Netscape Communications Corp., SAIC, Terisa Systems and VeriSign. SET is based, in **part** , on **encryption** technology from RSA **Data** Security.

"With SET, **consumers** and merchants will make convenient bankcard transactions in cyberspace as securely and easily as they...

26/3,K/14 (Item 11 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2003 The Gale Group. All rts. reserv.

04384161 Supplier Number: 46429987 (USE FORMAT 7 FOR FULLTEXT)
American Companies in Japans: SEMICONDUCTORS: MICROCHIP TECHNOLOGY, INC.
Japan-U.S. Business Report, v1996, n321, pN/A
June 1, 1996
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 68

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
...use of its KEELOQ secured unidirectional authentication algorithm for remote keyless entry. Using the KEELOQ **algorithm** , the **transmitter** provides an always changing and thus highly secure **encrypted** message. The transmitter **parts** now being sampled are the HCS300, the HCS301, the HCS200 and the HCS201. The 8...

26/3,K/15 (Item 12 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2003 The Gale Group. All rts. reserv.

03176847 Supplier Number: 44344095 (USE FORMAT 7 FOR FULLTEXT)
Public-key standard gets boost
Electronic Engineering Times, p4
Jan 10, 1994
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 545

... an automatic token system within a modem chip or smart card. The token scheme sets **keys** and **transfers** **encrypted** data as **part** of the modem handshake setup.

In addition to providing secure communications, Bidzos said, the token ...

26/3,K/16 (Item 13 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2003 The Gale Group. All rts. reserv.

02790798 Supplier Number: 43745685
Another Hitch for E-mail Security
Data Communications, p20
April, 1993
Language: English Record Type: Abstract
Document Type: Magazine/Journal; Trade

ABSTRACT:

...s (Redwood City, CA) products for handling the distribution and management of public e-mail **encryption** /decryption keys are **part** of a set of protocols approved by the Internet Engineering Task Force (IETF). However, the...

...Such standards are overdue. Under the IETF approved plan the sender uses a private encryption **key** and the **receiver** uses a public encryption key. The public and private keys must belong to the same...

26/3,K/17 (Item 14 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2003 The Gale Group. All rts. reserv.

02568222 Supplier Number: 43406867 (USE FORMAT 7 FOR FULLTEXT)
CRAY UNVEILS INNOVATIVE FPX2000 FAMILY OF FRAME RELAY FAST PACKET SWITCHING PRODUCTS
News Release, p1
Oct 29, 1992
Language: English Record Type: Fulltext
Document Type: Magazine/Journal; Trade
Word Count: 770

... DES Frame Relay Encryption Device provides securlry for users of public frame relay networks. It **encrypts** the **data portion** of **user** -selected frames using techniques established by the National Bureau of Standards. The entire process is...

26/3,K/18 (Item 15 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)
(c) 2003 The Gale Group. All rts. reserv.

02279617 Supplier Number: 42980440 (USE FORMAT 7 FOR FULLTEXT)
More Hearings On Export Ban On Data Encryption Software 05/08/92
Newsbytes, pN/A
May 8, 1992
Language: English Record Type: Fulltext
Document Type: Newswire; General Trade
Word Count: 570

(USE FORMAT 7 FOR FULLTEXT)
TEXT:
...pilgrimage to Capital Hill to ask again that Congress allow the export of software containing **data encryption** technology. Many foreign **buyers** demand that such **encryption** be a **part** of many programs and US law restricts the exports of such software.

26/3,K/19 (Item 1 from file: 47)
DIALOG(R)File 47:Gale Group Magazine DB(TM)
(c) 2003 The Gale group. All rts. reserv.

04637150 SUPPLIER NUMBER: 18874556 (USE FORMAT 7 OR 9 FOR FULL TEXT)
IBM to deliver framework for secure transactions. (new digital signature security framework to enable electronic commerce) (Company Business and Marketing)
Moeller, Michael; Kerstetter, Jim
PC Week, v13, n46, p6(1)

Nov 18, 1996
ISSN: 0740-1604 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 491 LINE COUNT: 00042

...ABSTRACT: technology that employs IBM's Cryptolopes, a digital version of certified mail, to deliver the **files** in an **encrypted** digital container. PQR **segments** a strong **encryption** key into individual **sections** represented by P, Q and R. The P and Q sections are **sent** to third- **party** **key** holders, the R segment accompanies the document as the encryption key. IBM plans to introduce...

26/3,K/20 (Item 2 from file: 47)
DIALOG(R)File 47:Gale Group Magazine DB(TM)
(c) 2003 The Gale group. All rts. reserv.

04579035 SUPPLIER NUMBER: 18624714 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Buying data bit by bit with microcash: new technology lets Internet users pay as they go. (digital cash systems) (includes a related article on Pacific Internet's WebCube Internet server) (PC Week Netweek) (Internet/Web/Online Service Information)
Kosiur, Dave
PC Week, v13, n34, pN3(2)
August 26, 1996
ISSN: 0740-1604 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1794 LINE COUNT: 00144

... steps of the transaction than Millicent's server.
In negotiations
In a novel approach, NetBill **encrypts** the goods sent, **partly** to ensure that delivery is acknowledged. Once the price has been negotiated between the customer...

...the customer is legitimate (for example, not using stolen tokens), only then will the merchant **send** a **key** to the **customer** for decrypting the purchased item.
This "certified delivery," as NetBill's developers call it, should...

26/3,K/21 (Item 3 from file: 47)
DIALOG(R)File 47:Gale Group Magazine DB(TM)
(c) 2003 The Gale group. All rts. reserv.

04226690 SUPPLIER NUMBER: 16844780 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Will your business be safe? (Internet security) (sidebar to: Building a Web Presence)
Reichard, Kevin
PC Magazine, v14, n9, p218(1)
May 16, 1995
ISSN: 0888-8507 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 750 LINE COUNT: 00059

... uses public-key technology to encrypt messages.
PGP combines public and secret keys from two **users** to **encrypt** a **file** or **part** of a mail message; you must have the public key of the **recipient** of an **encrypted** **file** for them to decrypt the file. A similar alternative is the MIT Kerberos authentication scheme...

26/3,K/22 (Item 4 from file: 47)

DIALOG(R)File 47:Gale Group Magazine DB(TM)
(c) 2003 The Gale group. All rts. reserv.

03991295 SUPPLIER NUMBER: 14803223 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Secure E-mail cheaply with software encryption.
Strauss, Paul
Datamation, v39, n23, p48(2)
Dec 1, 1993
ISSN: 1062-8363 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 1630 LINE COUNT: 00136

... cumbersome nature of RSA's fully public key, PEM and proprietary versions of public keys **encrypt** a **portion** of the message using the public key and the bulk of the message using a...

...4.0 of [EMC.sup.2] use this approach, says Fischer. In this case, the **sender** 's private **key** is encrypted with the public **key** and **transmitted** along with the message. The recipient's computer uses the public key to find the...

26/3,K/23 (Item 5 from file: 47)
DIALOG(R)File 47:Gale Group Magazine DB(TM)
(c) 2003 The Gale group. All rts. reserv.

03629492 SUPPLIER NUMBER: 11555740 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Data encryption, access-control devices tighten modem security.
Kramer, Matt
PC Week, v8, n47, p89(1)
Nov 25, 1991
ISSN: 0740-1604 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 786 LINE COUNT: 00064

... Reston, Va. Priced at $159, Tel/Assure provides file-transfer and general communications functions with **encrypted** traffic. To **encrypt data** , **users** also need a $399 data encryption board from Centel (the price includes the firm's...

...another Tel/Assure user armed with the necessary code. Users also have the option of **encrypting** the data **portion** of a message while leaving the header unscrambled, so a confidential message can be sent...

26/3,K/24 (Item 6 from file: 47)
DIALOG(R)File 47:Gale Group Magazine DB(TM)
(c) 2003 The Gale group. All rts. reserv.

03628921 SUPPLIER NUMBER: 11127592 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Messages in mathematically scrambled waves. (techniques for scrambling analog information such as telephone and television signals)
Peterson, Ivars
Science News, v140, n3, p37(2)
July 20, 1991
CODEN: SCNEB ISSN: 0036-8423 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 829 LINE COUNT: 00069

... set of numbers representing how many of each building block are present in the given **segment** . **Scrambling** these numbers produces a new, different waveform, which can then be sent as an **encrypted** **message** . The

receiver , who knows how the numbers were scrambled and which set of wavelets were used as...

26/3,K/25 (Item 7 from file: 47)
DIALOG(R)File 47:Gale Group Magazine DB(TM)
(c) 2003 The Gale group. All rts. reserv.

03622545 SUPPLIER NUMBER: 11434067 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Lotus Notes untangles red tape at tax department: switch from manual system lets agency answer taxpayers' questions in minutes. (work group software) (PC Week Special Report: Groupware supplement) (Case Study)
Garcia, Mary Ryan
PC Week, v8, n41, pS28(2)
Oct 14, 1991
ISSN: 0740-1604 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 1389 LINE COUNT: 00108

... from."
An extension of this concern is that of security. According to Lotus, Notes enables **users** to sign and **encrypt** mail **messages** or **parts** of messages. It allows users to have all incoming mail encrypted automatically. The product uses...

26/3,K/26 (Item 8 from file: 47)
DIALOG(R)File 47:Gale Group Magazine DB(TM)
(c) 2003 The Gale group. All rts. reserv.

03384333 SUPPLIER NUMBER: 08174766 (USE FORMAT 7 OR 9 FOR FULL TEXT)
How does Notes handle security? (security features in Lotus Notes work-group software) (related to 'Sky-high Notes')
Steinberg, Don
PC-Computing, v3, n3, p117(2)
March, 1990
ISSN: 0899-1847 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 908 LINE COUNT: 00070

...ABSTRACT: public key is included in the user's entry in the public directory, while the **encrypted** private key is **part** of the user's unique ID file. Servers 'challenge' each other with **encrypted** **messages** before exchanging **data** . **Users** can 'sign' and 'seal' documents using their encryption keys. A 'channel scrambling' feature encrypts all...

26/3,K/27 (Item 9 from file: 47)
DIALOG(R)File 47:Gale Group Magazine DB(TM)
(c) 2003 The Gale group. All rts. reserv.

03300222 SUPPLIER NUMBER: 07397806 (USE FORMAT 7 OR 9 FOR FULL TEXT)
A secret no more. (system security - includes related article on Data Encryption Standard)
Kerr, Susan
Datamation, v35, n13, p53(3)
July 1, 1989
ISSN: 1062-8363 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 1948 LINE COUNT: 00158

... into an unreadable jumble of characters and symbols. The key--essentially a string of digital **information** --allows **users** to

encode or decode a **message** . To date, key management has been the most complex and costly **part** of **encryption** . But newer electronic methods are simplifying the process.
Not always a Bargain
Most encryption users...

26/3,K/28 (Item 10 from file: 47)
DIALOG(R)File 47:Gale Group Magazine DB(TM)
(c) 2003 The Gale group. All rts. reserv.

03239041 SUPPLIER NUMBER: 07386744 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Products: encryption.
Bermar, Amy
PC Week, v6, n25, p108(1)
June 26, 1989
DOCUMENT TYPE: evaluation ISSN: 0740-1604 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT
WORD COUNT: 705 LINE COUNT: 00057

... an exclusive key-management system unique to each board, programmed during installation.
ISAC 3200 automatically **encrypts** and decrypts all **data** stored to disk. **Users** can also **encrypt parts** of a document from within an application using ISAC's application programming interface.
The product...

26/3,K/29 (Item 1 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2003 The Gale Group. All rts. reserv.

09332413 SUPPLIER NUMBER: 19161393 (USE FORMAT 7 OR 9 FOR FULL TEXT)
A question of symmetry? (encryption alternatives)
Hardy, Stephen M.
Journal of Electronic Defense, v20, n1, p42(4)
Jan, 1997
ISSN: 0192-429X LANGUAGE: English RECORD TYPE: Fulltext
WORD COUNT: 2829 LINE COUNT: 00231

... combinations can be applied to data in more than one way. Taking a message and **encrypting** all **parts** of it with a single key is called block encryption. If you attempt to increase...

...know the exact encryption key and how it was used in order to decrypt the **transmission** . Since the same **key** (or key combination) is used to encrypt and decrypt the message, substitution/permutation schemes such...

26/3,K/30 (Item 2 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2003 The Gale Group. All rts. reserv.

08310506 SUPPLIER NUMBER: 17781178 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Sun pushes for wider acceptance of SKIP. (Sun Microsystems' Simple Key Management for Internet Protocols) (Technology Information)
Rodriguez, Karen
CommunicationsWeek, n584, p5(1)
Nov 13, 1995
ISSN: 0746-8121 LANGUAGE: English RECORD TYPE: Fulltext; Abstract

WORD COUNT: 425 LINE COUNT: 00039

... Photuris, which directly competes with SKIP for security standards. SKIP and Photuris both address the **issue** of **key** management, a vital **part** of the **encryption** process that creates, distributes and authenticates public and private keys between communicating parties.Without this...

26/3,K/31 (Item 3 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2003 The Gale Group. All rts. reserv.

07990515 SUPPLIER NUMBER: 17140210 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Banks, government find an ally in packet encryption.
Wintrob, Suzanne
Computing Canada, v21, n11, p31(1)
May 24, 1995
ISSN: 0319-0161 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 522 LINE COUNT: 00046

...ABSTRACT: closet. There are two types of data encryption that can be used to protect corporate **data** . **Packet encryption** allows the **user** to individually **encrypt** a **packet** to be sent over a WAN; link encryption encrypts all data passing through a given link. The link encryption approach makes retrieval more difficult because the entire file is **encrypted** , instead of selective **portions** . Packet **encryption** allows only sensitive data to be encrypted, which is as little as 5% of the...

26/3,K/32 (Item 4 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2003 The Gale Group. All rts. reserv.

07759596 SUPPLIER NUMBER: 16736234 (USE FORMAT 7 OR 9 FOR FULL TEXT)
CRAY COMMUNICATIONS FRAME RELAY ENCRYPTOR WINS BEST OF SHOW AWARD
PR Newswire, p0330LA021
March 30, 1995
LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 533 LINE COUNT: 00045

... overcomes the security concerns of transporting mission-critical data over public frame relay facilities. By **encrypting** the **data portion** , or **user** selected frames using the techniques established by the National Bureau of Standards, the frame relay...

26/3,K/33 (Item 5 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2003 The Gale Group. All rts. reserv.

04609197 SUPPLIER NUMBER: 08616556 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Crimestoppers. (Software Review) (Visitec PC Boot, Computer Security PC Guard, PC Security Stoplock IV security software) (evaluation)
Kendrick, Nigel
PC User, n134, p83(3)
June 6, 1990
DOCUMENT TYPE: evaluation ISSN: 0263-5720 LANGUAGE: ENGLISH
RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 2732 LINE COUNT: 00204

... the system administrator to set up file access permissions. Instead, these are assigned by the **users** as they **scramble** their **individual data files** ; as **part** of the **scrambling** procedure, users enter the names or groups who should also be allowed to access the...

26/3,K/34 (Item 6 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2003 The Gale Group. All rts. reserv.

04064557 SUPPLIER NUMBER: 07702371 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Securing CD-ROMs and the microcomputer environment.
Ang, Soon; Straub, Detmar
Laserdisk Professional, v2, n4, p18(6)
July, 1989
ISSN: 0896-4149 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 2941 LINE COUNT: 00238

... the caller's number in a directory, and dials the number to reestablish communications.
DATA **ENCRYPTION**
Specific **sections** of CD-ROM disks containing sensitive information can be protected by requiring the user to...

...or privileges. This can be achieved using cryptography to impose different access restrictions on various **users** .
Cryptography involves **encryption** -- transforming **information** into unintelligible form (i.e., ciphertext) -- and decryption -- converting it to its original form (i...

26/3,K/35 (Item 7 from file: 148)
DIALOG(R)File 148:Gale Group Trade & Industry DB
(c)2003 The Gale Group. All rts. reserv.

03822670 SUPPLIER NUMBER: 07328091
Semicustom ICs put SBE into systems. (product announcement)
Costlow, Terry
Electronic Engineering Times, n524, p94(1)
Feb 6, 1989
DOCUMENT TYPE: product announcement ISSN: 0192-1541 LANGUAGE: ENGLISH RECORD TYPE: ABSTRACT

...ABSTRACT: semicustom ICs. The CPS-1 features six gate arrays and uses daughter boards to let **users** add data **encryption** or extra networking **parts** without decreasing performance. One of the board's most important gate arrays is the serial...

26/3,K/36 (Item 1 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2003 The Gale Group. All rts. reserv.

02223520 SUPPLIER NUMBER: 21136128 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Create a Windows NT virtual private network.(includes related articles on Windows Remote Access Service (RAS), and Advisor Tips) (Technology Tutorial)
Geralnik, Pablo
e-Business Advisor, v16, n9, p44(5)

Sept, 1998
LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 2407 LINE COUNT: 00180

... a Windows NT network, the administrator of the RAS server has the option of requiring **users** to use **encryption** for **data** (**information** being transferred). Logon and password passing is automatically **encrypted** . The client **part** of RAS is also referred to as Dial-up Networking. Once connected, you can work...

26/3,K/37 (Item 2 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02146246 SUPPLIER NUMBER: 20297031 (USE FORMAT 7 OR 9 FOR FULL TEXT)
E-mail messaging opens up. (Internet standards force vendors to open e-mail systems) (includes related articles on E-mail standards and S/MIME and PGP) (Internet/Web/Online Service Information) (Cover Story)
Rodriguez, Karen
Network, v13, n3, p34(6)
Feb, 1998
DOCUMENT TYPE: Cover Story LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 4754 LINE COUNT: 00391

... Message Access Protocol 4, or IMAP-4 (see below), has features to allow retrieval of **individual parts** of MIME- **encoded messages** .
POP-3 Post Office Protocol 3 is a client-side mail protocol designed to facilitate...

26/3,K/38 (Item 3 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02117692 SUPPLIER NUMBER: 19969595 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Ironside refines security, flexibility. (Ironside Technologies' Ironworks 1.4 electronic commerce software) (Product Announcement)
Greenemeier, Larry
MIDRANGE Systems, v10, n17, p25(1)
Oct 24, 1997
DOCUMENT TYPE: Product Announcement ISSN: 1041-8237 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 362 LINE COUNT: 00033

...ABSTRACT: software, which now offers multiple host support and bolstered security. The product allows users to **encrypt** a **portion** of or all of an applet. The new utility's usage extends to a variety of industries. Ironworks 1.4 offers optional **data encryption** for **data** transfers between Internet **users** and Ironworks servers, support for Netscape Navigator 4.x for Windows NT/95 and support...

26/3,K/39 (Item 4 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

02109735 SUPPLIER NUMBER: 19799952 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Put your personal data under lock and key. (McAfee Associates' PCCrypto

1.0.1 for Windows 3.1/95/NT encryption tool)(Security Advisor) (Software Review)(Column)(Evaluation)
Cobb, Michael
Databased Web Advisor, v15, n10, p72(4)
Oct, 1997
DOCUMENT TYPE: Column Evaluation ISSN: 1090-6436 LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1199 LINE COUNT: 00096

...ABSTRACT: archive rather than encrypting them individually. PCCrypto employs a tabbed-notebook layout and it allows **users** to **encrypt** and decrypt clipboard **information** that has been cut and pasted from both e-mail messages and documents. Users, therefore, are able to **encrypt** specific **portions** of these documents. The program, however, disallows users from automatically deleting plain text files that...
... the plain text data before it's encrypted, using the LZ77 compression algorithm.
PCCrypto lets **users** **encrypt** and decrypt clipboard **data** that's been cut and pasted from a document or e-mail message. This means you can **encrypt** just **part** of a document or an e-mail message. For example, the previous sentence turned into...

26/3,K/40 (Item 5 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2003 The Gale Group. All rts. reserv.

01910010 SUPPLIER NUMBER: 18032642 (USE FORMAT 7 OR 9 FOR FULL TEXT)
KARMA: the Knowledge Acquisition Reference Multimedia Aid. (a project that focuses on teaching students 'knowledge acquisition') (Technology Information)
Liebowitz, Jay; Letsky, Christine
T H E Journal (Technological Horizons In Education), v23, n7, p85(3)
Feb, 1996
ISSN: 0192-592X LANGUAGE: English RECORD TYPE: Fulltext; Abstract
WORD COUNT: 1751 LINE COUNT: 00153

... questions, and glossary terms accompany the first four sections. Navigation devices, various sounds, graphics and **user** -sensitive messages are **encoded** as **part** of KARMA.
The fifth section on "Models and Examples" currently provides audio dialogues with a...

26/3,K/41 (Item 6 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2003 The Gale Group. All rts. reserv.

01613712 SUPPLIER NUMBER: 14188929 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Make it real. (using authentication in network security)
Stallings, William
LAN Magazine, v8, n9, p105(6)
Sept, 1993
ISSN: 0898-0012 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 3799 LINE COUNT: 00295

... case of a dispute. A more efficient way of achieving the same results is to **encrypt** only a **portion** of the document. A minimal portion would include the sender's name, the receiver's...

...sequence number, and a checksum. If this portion of the message is encrypted with the **sender** 's private **key** , it serves as a signature that verities origin, content, and sequencing.
This encryption process does...

26/3,K/42 (Item 7 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

01581258 SUPPLIER NUMBER: 13310169 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Cray's frame relay. (Cray Communications introduces FPX2000 packet switches) (New Products)(Brief Article) (Product Announcement)
LAN Technology, v9, n2, p97(1)
Feb, 1993
DOCUMENT TYPE: Product Announcement ISSN: 1042-4695 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 251 LINE COUNT: 00019

TEXT:
...LAN and other traffic using flame relay or X.25. The FPX4802/DES Frame Relay **Encryption** device **encrypts** the **data portion** of **user** -selected flames. The encryption is transparent to the user. The device is available with a...

26/3,K/43 (Item 8 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

01581254 SUPPLIER NUMBER: 13310153 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Network laser printers. (Product Focus)(overview of three product introductions) (Brief Article)
Dorshkind, Brent
LAN Technology, v9, n2, p89(1)
Feb, 1993
DOCUMENT TYPE: Brief Article ISSN: 1042-4695 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 2497 LINE COUNT: 00196

... LAN and other traffic using frame relay or X.25. The FPX4802/DES Frame Relay **Encryption** device **encrypts** the **data portion** of **user** -selected frames. The encryption is transparent to the user. The device is available with a...

26/3,K/44 (Item 9 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)

01581253 SUPPLIER NUMBER: 13309699 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Crowning printer. (Network Laser Printers)(Product Focus) (Product Announcement)
Dorshkind, Brent
LAN Technology, v9, n2, p89(2)
Feb, 1993
DOCUMENT TYPE: Product Announcement ISSN: 1042-4695 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 2497 LINE COUNT: 00196

... LAN and other traffic using frame relay or X.25. The FPX4802/DES Frame Relay **Encryption** device encrypts the **data portion** of **user** -selected frames. The encryption is transparent to the user. The device is available with a...

26/3,K/45 (Item 10 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2003 The Gale Group. All rts. reserv.

01513652 SUPPLIER NUMBER: 12146996 (USE FORMAT 7 OR 9 FOR FULL TEXT)
More hearings on export ban on data encryption software. (Congress)
McCormick, John
Newsbytes, NEW05080018
May 8, 1992
LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 612 LINE COUNT: 00049

TEXT:
...pilgrimage to Capital Hill to ask again that Congress allow the export of software containing **data encryption** technology. Many foreign **buyers** demand that such **encryption** be a **part** of many programs and US law restricts the exports of such software.

26/3,K/46 (Item 11 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2003 The Gale Group. All rts. reserv.

01451344 SUPPLIER NUMBER: 11287630 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Safe and secure. (administrative plans and products provide maximum LAN protection) (includes a related article on the vulnerability of private information and on the CSI Security Conference)
Stephenson, Peter
LAN Magazine, v6, n9, p34(7)
Sept, 1991
ISSN: 0898-0012 LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT; ABSTRACT
WORD COUNT: 5062 LINE COUNT: 00404

... are used to where they are stored. As a general practice, any data leaving an **individual** LAN should be **encrypted** . If you pass **data** between a LAN and a mainframe, for example, you should consider **encrypting** it.
BETWEEN NETWORK **SEGMENTS**
Establishing security between network systems is a bit trickier because an implicit assumption is that...

26/3,K/47 (Item 12 from file: 275)
DIALOG(R)File 275:Gale Group Computer DB(TM)
(c) 2003 The Gale Group. All rts. reserv.

01178422 SUPPLIER NUMBER: 04427349 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Electronic mail products.
Communications News, v23, p40(7)
Sept, 1986
LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
WORD COUNT: 5283 LINE COUNT: 00438

... in the message, encryption is turned on and off as desired. With

Safe-Mail, the **user** is able to **encrypt** **portions** of the **message** . Safe-Mail's ability to encrypt packets of data provides an advantage as users must...

```
File   2:INSPEC 1969-2003/Jul W3
         (c) 2003 Institution of Electrical Engineers
File   6:NTIS 1964-2003/Jul W4
         (c) 2003 NTIS, Intl Cpyrght All Rights Res
File   8:Ei Compendex(R) 1970-2003/Jul W3
         (c) 2003 Elsevier Eng.  Info. Inc.
File  34:SciSearch(R) Cited Ref Sci 1990-2003/Jul W4
         (c) 2003 Inst for Sci Info
File  35:Dissertation Abs Online 1861-2003/Jun
         (c) 2003 ProQuest Info&Learning
File  65:Inside Conferences 1993-2003/Jul W4
         (c) 2003 BLDSC all rts. reserv.
File  94:JICST-EPlus 1985-2003/Jul W3
         (c)2003 Japan Science and Tech Corp(JST)
File  95:TEME-Technology & Management 1989-2003/Jul W2
         (c) 2003 FIZ TECHNIK
File  99:Wilson Appl. Sci & Tech Abs 1983-2003/Jun
         (c) 2003 The HW Wilson Co.
File 111:TGG Natl.Newspaper Index(SM) 1979-2003/Jul 31
         (c) 2003 The Gale Group
File 144:Pascal 1973-2003/Jul W3
         (c) 2003 INIST/CNRS
File 202:Info. Sci. & Tech. Abs. 1966-2003/Jul 31
         (c) Information Today, Inc
File 233:Internet & Personal Comp. Abs. 1981-2003/Jul
         (c) 2003 Info. Today Inc.
File 266:FEDRIP 2003/Jun
         Comp & dist by NTIS, Intl Copyright All Rights Res
File 434:SciSearch(R) Cited Ref Sci 1974-1989/Dec
         (c) 1998 Inst for Sci Info
File 483:Newspaper Abs Daily 1986-2003/Jul 31
         (c) 2003 ProQuest Info&Learning
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
         (c) 2002 The Gale Group
? ds

Set     Items   Description
S1    2406897   KEY? ? OR CIPHER? OR CYPHER? OR ALGORITHM?
S2      65179   S1(3N)(SEND??? ? OR SENT OR TRANSMIT? OR TRANSMIS? OR TRAN-
              SFER? OR XFER? OR DELIVER? OR ISSUE? ? OR ISSUING OR ISSUANCE?
               OR RECEIV? OR RECEIPT? ? OR RECEPTION?)
S3     473140   CIPHER? OR CYPHER? OR ENCIPHER? OR ENCYPHER? OR ENCRYPT? OR
              SCRAMBL? OR ENCOD???? ?
S4      33907   S3(3N)(DATA OR INFORMATION OR PACKET? ? OR MESSAG??? ? OR -
              FILE OR FILES OR CONTENT)
S5        793   S4(3N)(USER? OR CLIENT? OR RECIPIENT? OR BUYER? OR RECEIVE-
              R? OR PATRON? OR PURCHASER? OR CONSUMER? OR CUSTOMER? OR SHOP-
              PER? OR SUBSCRIBER?)
S6         35   S4(3N)(REQUEST?R? ? OR ESHOPPER? OR PARTICIPANT? OR MEMBER?
               ? OR NETIZEN?)
S7        127   S4(3N)(INDIVIDUAL? ? OR PERSON? ? OR PARTY)
S8         56   S2 AND S5:S7
S9         23   S8/2000:2003
S10        33   S8 NOT S9
S11        26   RD (unique items)
S12        23   S11 NOT PHASE()SHIFT?
S13       574   S2(3N)(USER? OR CLIENT? OR RECIPIENT? OR BUYER? OR PATRON?
              OR PURCHASER? OR CONSUMER? OR CUSTOMER? OR SHOPPER? OR SUBSCR-
              IBER?)
S14       217   S2(3N)(REQUEST?R? ? OR ESHOPPER? OR PARTICIPANT? OR MEMBER?
               ? OR NETIZEN? OR INDIVIDUAL? ? OR PERSON? ? OR PARTY)
```

S15 22 S13:S14 AND S4
S16 7 S15/2000:2003
S17 15 S15 NOT S16
S18 34 S17 OR S12
S19 34 S18 NOT (PHASE()SHIFT? OR RADIO()RECEIV?)
S20 31 RD (unique items)
? t20/7/all

20/7/1 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

5122988 INSPEC Abstract Number: B9601-6120B-059, C9601-6130S-056
Title: On key storage in secure networks
Author(s): Dyer, M.; Fenner, T.; Frieze, A.; Thomason, A.
Author Affiliation: Sch. of Comput. Studies, Leeds Univ., UK
Journal: Journal of Cryptology vol.8, no.4 p.189-200
Publication Date: Autumn 1995 Country of Publication: USA
CODEN: JOCREQ ISSN: 0933-2790
Language: English Document Type: Journal Paper (JP)
Treatment: Theoretical (T)
Abstract: We consider systems where the keys for **encrypting messages** are derived from the pairwise intersections of sets of private **keys issued** to the **users** . We give improved bounds on the storage requirements of systems of this type for secure communication in a large network. (9 Refs)
Subfile: B C

20/7/2 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

5039194 INSPEC Abstract Number: B9510-6120B-056, C9510-6130S-036
Title: Low exponent attack against elliptic curve RSA
Author(s): Kurosawa, K.; Okada, K.; Tsujii, S.
Author Affiliation: Dept. of Electr. & Electron. Eng., Tokyo Inst. of Technol., Japan
Conference Title: Advances in Cryptology - ASIACRYPT'94. 4th International Conference on the Theory and Applications of Cryptology. Proceedings p.376-83
Editor(s): Pieprzyk, J.; Safavi-Naini, R.
Publisher: Springer-Verlag, Berlin, Germany
Publication Date: 1995 Country of Publication: West Germany xii+430 pp.
ISBN: 3 540 59339 X
Conference Title: Advances in Cryptology - ASIACRYPT '94. 4th International Conference on the Theory and Applications of Cryptology
Conference Sponsor: Univ. Wollongong
Conference Date: 28 Nov.-1 Dec. 1994 Conference Location: Wollongong, NSW, Australia
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T)
Abstract: Hastad (1985) has shown that low exponent RSA is not secure if the same **message** is **encrypted** to several **receivers** . This is true even if a timestamp is used for each receiver. For example, let e=3. Then, if the number of receivers =7, the eavesdropper can find the plaintext from the seven **ciphertexts** of each **receiver** . This paper shows that elliptic curve RSA is not secure in the same scenario. It is shown that the KMOV

scheme and Demytko's scheme are not secure if e=5, n>or=2/sup 1024/ and the number of receivers =428. In Demytko's scheme, e can take the value of 2. In this case, this system is not secure if the number of receivers =11 for n >or=2/sup 175/. (6 Refs)
Subfile: B C

20/7/3 (Item 3 from file: 2)
DIALOG(R)File 2:INSPEC

03926995 INSPEC Abstract Number: C91048132
Title: Key distribution system using ID-related information directory suitable for mail systems
Author(s): Tanaka, K.; Okamoto, E.
Author Affiliation: C & C Inf. Technol. Res. Lab., NEC Corp., Kawasaki, Japan
Conference Title: SECURICOM 90. 8th Worldwide Congress on Computer and Communications Security and Protection p.115-22
Publisher: SEDEP, Paris, France
Publication Date: 1990 Country of Publication: France 306 pp.
Conference Date: 14-16 March 1990 Conference Location: Paris, France
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: A key distribution system suitable for mail systems is presented. The system uses a public directory, which contains each user's ID-related information, but is strong against forgery. A **sender** generates **key** and **key** information which depends on the **receiver** , and **sends** the **key** information along with the **encrypted message** . Only the **receiver** whom the sender intended can obtain the common key from the key information, and decrypt the message. He can also convince himself of the sender being authentic. Since a random number is used in generation of a key and its information, keys are different in every mail. The paper further discusses the implementation of the proposed system on a present personal computer network. (8 Refs)
Subfile: C

20/7/4 (Item 4 from file: 2)
DIALOG(R)File 2:INSPEC

02305585 INSPEC Abstract Number: B84048119, C84040431
Title: Applying data security to the videotex industry
Author(s): Hall, D.; Ritter, W.; Poletto, E.
Conference Title: World Videotex Report. Proceedings of Videotex '83 and Videotex Europe p.323-33
Publisher: Online Publications, Northwood Hills, UK
Publication Date: 1984 Country of Publication: UK xv+866 pp.
ISBN: 0 86353 002 8
Conference Date: 22-29 June 1983 and Nov. 1983 Conference Location: New York, NY, USA and Amsterdam, Netherlands
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: Utilization of the **Data Encryption** Standard (DES) is envisioned for securing sensitive data transmission in the videotex industry. Requirements for a secure module to be attached to a videotex host system are described and a method is developed for secure session logon using a randomly-generated **key** which requires no **transmission** of

the **subscriber** 's secret key. Home banking in South Florida is the first expected application of this scheme. (6 Refs)
Subfile: B C

20/7/5 (Item 5 from file: 2)
DIALOG(R)File 2:INSPEC

01985617 INSPEC Abstract Number: B83008627
Title: Embedding data in speech using scrambling techniques
Author(s): Steele, R.; Vitello, D.
Author Affiliation: Crawford Hill Lab., Bell Labs., Holmdel, NJ, USA
Conference Title: Proceedings of ICASSP 82. IEEE International Conference on Acoustics, Speech and Signal Processing p.1801-4
Publisher: IEEE, New York, NY, USA
Publication Date: 1982 Country of Publication: USA 3 vol. 2104 pp.
U.S. Copyright Clearance Center Code: CH 1746-7/82/0000 - 1801 $ 00.75
Conference Sponsor: IEEE
Conference Date: 3-5 May 1982 Conference Location: Paris, France
Language: English Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: A method of embedding data into speech signals is proposed. The speech signal is **scrambled** using the **data** as the **scrambling key** , while the **receiver** adopts the role of a code breaker. By judicious choice of scrambling **algorithm** the **receiver** can be made to break the code at every attempt. The authors found that 126 b/s can be transmitted without error over a channel whose additive noise is only 10 dB below the mean square value of the speech signal. (2 Refs)
Subfile: B

20/7/6 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

04651588 E.I. No: EIP97033577212
Title: Optimal quantization for finite-state channels
Author: Duman, Tolga M.; Salehi, Masoud
Corporate Source: Northeastern Univ, Boston, MA, USA
Source: IEEE Transactions on Information Theory v 43 n 2 Mar 1997. p 758-765
Publication Year: 1997
CODEN: IETTAW
Language: English
Document Type: JA; (Journal Article) Treatment: T; (Theoretical)
Journal Announcement: 9705W2
Abstract: Optimal scalar quantizer design for transmission over a finite-state channel is considered. The objective is to minimize the mean-squared error when the channel is in the normal mode of operation, while guaranteeing a minimum fidelity when the channel is in the 'bad' state. An optimal quantizer design algorithm for the general case where noisy state information is available both at the receiver and at the transmitter is derived. It is shown that using mixed strategies is necessary in order to achieve the optimal performance. Finally, the case where the observation is noisy is considered and it is shown that the optimal scheme in this case is to apply the algorithm for the 'no observation noise' to the mean-squared estimate of the desired random variable from the noisy data. (Author abstract) 7 Refs.

20/7/7 (Item 2 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

04332032 E.I. No: EIP96013010784
Title: New subliminal channel based on Fiat-Shamir's signature scheme
Author: Chen, Chien-Yuan; Chang, Chin-Chen; Yang, Wei-Pang
Corporate Source: Natl Chiao Tung Univ, Hsinchu, Taiwan
Source: Journal of the Chinese Institute of Engineers, Transactions of the Chinese Institute of Engineers,Series A/Chung-kuo Kung Ch'eng Hsuch K'an v 18 n 6 Nov 1995. p 867-872
Publication Year: 1995
CODEN: JCIEEZ ISSN: 0253-3839
Language: English
Document Type: JA; (Journal Article) Treatment: T; (Theoretical)
Journal Announcement: 9603W3
Abstract: This paper constructs a subliminal channel in a RSA-like variant of the Fiat-Shamir signature scheme to transfer any secret information. The proposed subliminal channel, unlike that in El-Gamal signature scheme, can avoid the serious shortcoming that a subliminal receiver can undetectably forge a signer's signature. In addition, our channel also overcomes almost all shortcomings from which the subliminal channel in El-Gamal signature scheme suffer. (Author abstract) 10 Refs.

20/7/8 (Item 3 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

04082817 E.I. No: EIP95022584505
Title: Code timing estimation in a near-far environment for direct-sequence code-division multiple-access
Author: Smith, Ronald F.; Miller, Scott L.
Corporate Source: Univ of Florida, Gainesville, FL, USA
Conference Title: Proceedings of the 1994 IEEE MILCOM. Part 1 of 3
Conference Location: Long Branch, NJ, USA Conference Date: 19941002-19941005
Sponsor: IEEE
E.I. Conference No.: 42512
Source: IEEE MILCOM v 1 1994. IEEE, Piscataway, NJ, USA,94CH3400-9. p 47-51
Publication Year: 1994
CODEN: 001918
Language: English
Document Type: CA; (Conference Article) Treatment: T; (Theoretical)
Journal Announcement: 9504W4
Abstract: An adaptive receiver structure is considered for obtaining timing information for a direct-sequence code-division multiple-access (CDMA) communication network operating in a near-far environment. The receiver consists of a chip matched filter followed by an adaptive equalizer. By using a simple channel-access protocol, the timing information for a new system user can be extracted from the weights of the adaptive equalizer. In order to obtain this timing information, the receiver only requires knowledge of the spreading code of the new user. A Maximum-Likelihood (ML) estimation algorithm is given based on several simplistic assumptions on the statistical properties of the adaptive filter tap weights. Several different CDMA environments were simulated, and the performance of the ML estimation algorithm is presented. These results show that even though simplistic assumptions were used in the derivation of the ML estimation **algorithm** , this **receiver** structure is applicable to extracting timing information for a direct-sequence CDMA system operating

in a near-far environment. (Author abstract) 7 Refs.

20/7/9 (Item 4 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

04069732 E.I. No: EIP95022559675
Title: Soft-decision multistage decoding of multilevel-coded quaternary partial-response signals
Author: Olcer, Sedat
Corporate Source: IBM Research Div, Ruschlikon, Switz
Conference Title: Proceedings of the 1994 IEEE International Symposium on Information Theory
Conference Location: Trodheim, Norw Conference Date: 19940627-19940701
Sponsor: IEEE
E.I. Conference No.: 42405
Source: IEEE International Symposium on Information Theory - Proceedings 1994. IEEE, Piscataway, NJ, USA,94CH3467-8. 473p
Publication Year: 1994
CODEN: 001793
Language: English
Document Type: CA; (Conference Article) Treatment: T; (Theoretical)
Journal Announcement: 9504W3
Abstract: This paper deals with multilevel coding and concatenated soft-decision multistage decoding for quaternary dicode partial-response systems. Time-interleaved quaternary symbols are transmitted with precoding over the dicode channel. A single level of coding is assumed, whereby only the less significant bits of the transmitted quaternary symbols are encoded. In the receiver, an inner decoder computes approximate log-likelihood ratios for the less significant bits of the quaternary symbols input to the precoded partial-response channel by a new, reduced two-state, soft-output Viterbi decoding algorithm. With sufficient interleaving, the log-likelihood ratios represent the appropriate metrics for soft-decision decoding by an outer multistage decoder. Real coding gains over uncoded transmission with optimum maximum-likelihood sequence decoding were determined by simulation. Results are presented for various multilevel codes based on binary convolutional or Reed-Muller block codes. This scheme exhibits low decoding complexity and allows high-rate codes that achieve real coding gains of 3 to 4 dB. (Author abstract) 10 Refs.

20/7/10 (Item 5 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

04056561 E.I. No: EIP95022546526
Title: Method for constructing a group-oriented cipher system
Author: Lin, Chu-Hsing; Chang, Chin-Chen
Corporate Source: Tung Hai Univ, Taichung, Taiwan
Source: Computer Communications 17 11 Nov 1994. p 805-808
Publication Year: 1994
CODEN: COCOD7
Language: English
Document Type: JA; (Journal Article) Treatment: G; (General Review)
Journal Announcement: 9504W2
Abstract: In this research note, we propose a solution to the problem of generalized group-oriented cryptography. By applying the scheme presented one can send a confidential message to a group of users such that the message can be revealed only when the specified members cooperatively work together. The organization and policy of the target group does not need to

be known by the **sender** ; only the public **keys** of **users** in the group are needed. The scheme presented is quite practical, and can be used in a large group-oriented network. (Author abstract) 10 Refs.

20/7/11 (Item 6 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

02644375 E.I. Monthly No: EIM8809-048243
Title: ENHANCED TERMINAL TO SUPPORT A RELIABLE 64 kb/s SERVICE.
Author: Mahajan, Om P.
Corporate Source: AT&T Bell Lab, Holmdel, NJ, USA
Conference Title: IEEE/IEICE Global Telecommunications Conference 1987 - Conference Record.
Conference Location: Tokyo, Jpn Conference Date: 19871115
Sponsor: IEEE, Communications Soc, New York, NY, USA; Inst of Electronics, Information and Communication Engineers of Japan, Tokyo, Jpn; Foundation for Advancement of Int Science
E.I. Conference No.: 11418
Source: Publ by Ohmsha Ltd, Tokyo, Jpn. Available from IEEE Service Cent (Cat n 87CH2520-5), Piscataway, NJ, USA p 1121-1124
Publication Year: 1987
ISBN: 4-274-03188-8
Language: English
Document Type: PA; (Conference Paper)
Journal Announcement: 8809
Abstract: The author proposes an enhanced transmission terminal, incorporating data scrambling, to support 64 kb/s service over an existing digital network. The scrambling will allow continued use of in-band control codes (loopback codes, network failure codes, etc.) for service maintenance, and at the same time prevent user data from accidentally causing a loopback or simulating a failure **message** . By incorporating a **scrambling** algorithm in the **customer** premises equipment, no modifications are needed in the network to support the 64 kb/s service. 4 refs.

20/7/12 (Item 7 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

01500025 E.I. Monthly No: EI8403020744 E.I. Yearly No: EI84029250
Title: CRYPTOSYSTEM USING THE MASTER KEY FOR MULTI-ADDRESS COMMUNICATION.
Author: Koyama, Kenji
Corporate Source: Nippon Telegraph & Telephone Public Corp, Musashino Electrical Communication Lab, Musashino, Jpn
Source: Systems - Computers - Controls v 13 n 5 Sep-Oct 1982 p 36-46
Publication Year: 1982
CODEN: SYCCBB ISSN: 0096-8765
Language: ENGLISH
Journal Announcement: 8403
Abstract: A new cryptosystem using a master key as a security system in multi-address communication is proposed. In the master **key** system the **sender** encrypts the message with a master key that can be applied in common to the personal keys of the set of addresses and the regular **receivers** decrypt the **encrypted message** by personal keys. The encrypt algorithm used is the RSA public-key cryptosystem. The existence condition and the derivation method of the master key have already been presented for the key in the narrow sense, i. e. , the exponent key in the RSA method. In

order to apply the method to multi-address communication, the master key in the wider sense is analyzed and derived, including the modulus master key. Multiple crypto communication using a master key in the wide sense is formulated. It is shown that secret multi-address communication and multi-address digital signature are possible, and the actual protocols are presented. 8 refs.

20/7/13 (Item 1 from file: 34)
DIALOG(R)File 34:SciSearch(R) Cited Ref Sci

04580391 Genuine Article#: BE66E Number of References: 6
Title: LOW EXPONENT ATTACK AGAINST ELLIPTIC CURVE RSA
Author(s): KUROSAWA E; OKADA K; TSUJII S
Corporate Source: TOKYO INST TECHNOL,FAC ENGN,DEPT ELECT & ELECTRENGN,MEGURO KU,2-12-1 OOKAYAMA/TOKYO 152//JAPAN/; CHUO UNIV,DEPT INFORMAT SYST ENGN,BUNKYO KU/TOKYO 112//JAPAN/
Journal: LECTURE NOTES IN COMPUTER SCIENCE, 1995, V917, P376-383
ISSN: 0302-9743
Language: ENGLISH Document Type: ARTICLE
Abstract: Hastad showed that low exponent RSA is not secure if the same **message** is **encrypted** to several **receivers** . This is true even if time-stamp is used for each receiver. For example, let e = 3. Then if the number of receivers = 7, the eavesdropper can find the plaintext from the seven **ciphertexts** of each **receiver** .

This paper shows that elliptic curve RSA is not secure in the same scenario. It is shown that the KMOV scheme and Demytko's scheme are not secure if e = 5, n greater than or equal to 2(1024) and the number of receivers = 428. In Demytko's scheme, e can take the value of 2. In this case, this system is not secure if the number of receiver = 11 for n 2 greater than or equal to 2(175).

20/7/14 (Item 1 from file: 95)
DIALOG(R)File 95:TEME-Technology & Management

01348996 I99101223300
On the key escrow system without key exchange
Yung-Cheng Lee; Chi-Sung Laih
Dept. of Electr. Eng., Nat. Cheng Kung Univ., Tainan, RC
Computers and Electrical Engineering, v25, n4, pp279-290, 1999
Document type: journal article Language: English
Record type: Abstract
ISSN: 0045-7906

ABSTRACT:
The key escrow system bridges the gap between privacy and protection against criminal behavior. We propose a new key escrow system (NKES) and a partial key escrow system (PKES). Both of the systems have the advantages such as the users need not to perform **key** exchange beforehand, the **sender** always generates a true law enforcement access field whenever the information is encrypted, and the law enforcement access field cannot be successfully forged. Beside these advantages, the partial key escrow system has a delay recovery property, which is essential for user privacy.

20/7/15 (Item 2 from file: 95)

DIALOG(R)File 95:TEME-Technology & Management

01301897 E99040209249
Kein E-Commerce ohne E-Money. Elektronische Zahlungskonzepte - Ueberblick und Bewertung
Zangeneh, K
GMD Darmstadt, D
Computerwoche Extra, v91, n2, pp20-21,23,27, 1999
Document type: journal article Language: German
Record type: Abstract
ISSN: 0935-1310

ABSTRACT:
Die wachsende Bedeutung des E-Commerce wird die Entwicklung elektronischer Bezahlsysteme beschleunigen. Vor diesem Hintergrund werden im Artikel die existierenden elektronischen Zahlungskonzepte vorgestellt und bewertet. In Betracht kommen dabei folgende Bezahlsysteme: SET (Secure Electronic Transactions), CyberCash, GeldKarte, Ecash, CAFE, Milicent und Mondex. Sie unterscheiden sich zum Teil erheblich in technischen, betriebswirtschaftlichen und organisatorischen Aspekten, die dem Autor als Kriterien zur Bewertung eines Bezahlsystems dienen. Die technischen Kriterien setzten sich aus den bekannten Kriterien zusammen, die anhand von Sicherheitsmechanismen durch Einsatz von kryptographischen Mitteln zu verwirklichen sind. Hierzu gehoeren beispielsweise Verfuegbarkeit und Zuverlaessigkeit des gesamten Systems, Vertraulichkeit der Daten sowie Authentizitaet aller Beteiligten. Die betriebswirtschaftlichen Kriterien wiederum umfassen alle mit einem Zahlungssystem zusammenhaengenden Gebuehren, Transaktionskosten und Provisionsanteile. Die Reihenfolge der beiden Aktionen 'Geldtransfer' und 'Warenlieferung' in einer Geschaeftstransaktion zaehlt zu den organisatorischen Kriterien. Abschliessend betrachtet muss man sagen, dass elektronische Be-zahlsysteme heute noch am Beginn ihrer Entwicklung stehen. Niemand weiss, wohin die Reise geht. Bislang konnte sich noch kein Standard herauskristallisieren. Zumindest SET scheint aber ein geeigneter Kandidat fuer Kre-ditkartensysteme im Internet zu sein. Ansonsten wird die Macht des Faktischen wirken - die Akzeptanz bei Finanzinstituten, Verkaeufern und Kaeufern. Deshalb ist in naechster Zeit mit einem Shake-out - insbesondere inkompatibler beziehungsweise nur schwer integrierbarer Systeme - zu rechnen.

20/7/16 (Item 3 from file: 95)
DIALOG(R)File 95:TEME-Technology & Management

01295023 E99030867261
Ausweiskontrolle. Sichere Web-to-Host-Loesungen realisieren
Lebrecht, G-C
ICOM Informatique Deutschland, Muenchen, D
net - Zeitschrift fuer Kommunikationsmanagement, v53, n3, pp78-80, 1999
Document type: journal article Language: German
Record type: Abstract
ISSN: 0947-4765

ABSTRACT:
Verschiedene Sicherheitsstufen und -konzepte zur Abwicklung geschaeftlicher Transaktionen ueber Intra-, Extra- bzw. Internet werden vorgestellt. Die erste Stufe umschreibt mit der Authentifizierung die Berechtigungskontrolle beim Zugriff auf einen Webserver, z.B. mittels Benutzer-ID, Passwort oder durch biometrischen Nachweis (Fingerabdruck etc.). Die naechste Stufe ist

die Autorisierung - hier wird der Zugang zu bestimmten Bereichen des Webservers z.B. durch den Einsatz von Firewalls geregelt. Das wirksamste Sicherheitskonzept folgt in der dritten Stufe mit der Verschluesselung (verschluesselte Daten koennen nur durch einen bestimmten Schluessel wieder lesbar gemacht werden). Alle drei Konzepte werden vorgestellt und tabellarisch miteinander verglichen.

20/7/17 (Item 4 from file: 95)

01172470 E98010166261
Angriffe abwehren. Schutzmassnahmen fuer Corporate Networks
Mueller, R
debis Systemhaus, Leinfelden-Echterdingen, D
net - Zeitschrift fuer Kommunikationsmanagement, v51, n12, pp44-46, 1997.
Document type: journal article Language: German
Record type: Abstract
ISSN: 0947-4765

ABSTRACT:
Unternehmenseigene Netze zur Informationsverarbeitung (Corporate Networks) stellen ein nicht zu unterschaetzendes Sicherheitsrisiko dar. Eine Reihe von Sicherheitsmechanismen und Massnahmen gegen aktive und passive Eingriffe in vernetzte Systeme werden vorgestellt. Hierzu zaehlen Sicherheitsdienste wie z.B. Authentisierung, Vertraulichkeit oder Datenintegritaet, deren praktischer Einsatz als Massnahmen gegen aktive und passive Angriffe verdeutlicht wird. Am Beispiel des debis-Netzes wird ein sicherer Zugang mit bestimmten Schutzmechanismen konkret erlaeutert.

20/7/18 (Item 5 from file: 95)

01065899 I96121282320
Entrust: the key to corporate data security
(Entrust: Der Schluessel fuer die Datensicherung)
O'Higgins, B
Telesis, v31, n101, pp42-54, 1996
Document type: journal article Language: English
Record type: Abstract
ISSN: 0040-2710

ABSTRACT:
The advent of client/server computing, growing corporate use of World Wide Web technology, and the resulting openness of electronic transactions are fueling a need for network security solutions that is more pressing than ever before. In addressing this need, Northern Telecom (Nortel) called on more than 15 years of leadership in cryptographic technology to develop the Entrust family of products: a unique suite of public-key security management tools that is rapidly gaining acceptance from some of the world's largest corporations. Indeed, with more than 100 companies, including IBM, Microsoft, Hewlett-Packard and Control Data Systems, signing on to Entrust since it was launched 18 months ago, Entrust is now emerging as the de facto standard for public-key management and a critical enabler of secure electronic commerce.

20/7/19 (Item 6 from file: 95)

DIALOG(R)File 95:TEME-Technology & Management

00991699 I96058063230
Combinatorial bounds and design of broadcast authentication
(Kombinatorische Grenzen und Entwurf von Uebertragungsechtheit)
Fujii, H; Kachen, W; Kurosawa, K
Dept. of Electr. & Electron. Eng., Tokyo Inst. of Technol., Japan
IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vE79-A, n4, pp502-506, 1996
Document type: journal article Language: English
Record type: Abstract
ISSN: 0916-8508

ABSTRACT:
This paper presents a combinatorial characterization of broadcast authentication in which a transmitter broadcasts u messages e(ind 1)(s),...,e(ind u)(s) to authenticate a source state s to all n receivers so that any k receivers cannot cheat any other receivers, where e(ind i) is a **key** . Suppose that each **receiver** has l **keys** . First, we prove that k<l if u<n. Then we show an upper bound of n such that n<or=u(u-1)/l(l-1) for k=l-1 and n<or=((ind (l)k)/(exp u))/((ind (l)k)/(exp l))+((ind (l)k)/(exp u)) for k<l-1. Further, a scheme for k=l-1 which meets the upper bound is presented by using a BIBD and a scheme for k<l-i such that n=((ind (l)k)/(exp u))/((ind (l)k)/(exp l)) is presented by using a Steiner system. Some other effcient schemes are also presented.

20/7/20 (Item 7 from file: 95)
DIALOG(R)File 95:TEME-Technology & Management

00874703 E95031215278
Schweizer Forscher entwickelt neue Verschluesselungsmethode. Problem der Datensicherheit soll prinzipiell geloest sein
Weber, F
Computerwoche, v22, n10, pp67-68, 1995
Document type: journal article Language: German
Record type: Abstract
ISSN: 0170-5121

ABSTRACT:
Beim Schutz elektronischer Daten vor unberechtigtem Zugriff werden Verschluesselungssysteme eingesetzt. Das theoretisch vollkommene System hat aber einen grossen Haken. Wenn Sender und Empfaenger der Botschaft den Schluessel untereinander austauschen muessen, besteht das Risiko, dass er unterwegs in falsche Haende geraet. Der junge Schweizer Informatiker Ueli Maurers hat ein System entwickelt, das den genannten Haken nicht mehr hat. Dabei wird ein Schluessel verwendet, der vom Sender und Empfaenger nicht mehr gegenseitig ausgetauscht, sondern an Ort und Stelle jeweils konstruiert werden muss. Damit beide zum gleichen Resultat kommen, brauchen sie eine gemeinsame Datenquelle. Diese Quelle kann ein Satellit sein, der Zufallszahlen aussendet, die jedermann empfangen kann. Der Sender im Satellit wird so schwach eingestellt, dass auf der Erde kein fehlerfreier Empfang moeglich ist. Damit die beiden Kommunikationspartner auf einen gemeinsamen Schluessel kommen, unterteilen Sender und Empfaenger ihre empfangenen Signale in Gruppen und eruieren gegenseitig, bei welchen dieser Gruppen sie Uebereinstimmung haben. Alle anderen Gruppen werden aus den weiteren Betrachtungen ausgeschlossen. Sie erhalten so immer kuerzere Zahlenfolgen, die sich immer aehnlicher sind. Am Schluss stimmen die Resultate exakt ueberein und koennen somit als geheimer Schluessel dienen.

20/7/21 (Item 8 from file: 95)
DIALOG(R)File 95:TEME-Technology & Management

00874702 E95031216278
Wie man einen unangreifbaren geheimen Schluessel generiert. Abhoeren nuetzt nichts
anonym
Computerwoche, v22, n10, pp68-69, 1995
Document type: journal article Language: German
Record type: Abstract
ISSN: 0170-5121

ABSTRACT:
Durch ein neues Verfahren zur Verschluesselung von elektronischen Daten wird ein Chiffrierschluessel verwendet, der zwischen dem Sender und Empfaenger nicht ausgetauscht werden muss. Die Unangreifbarkeit dieses Schluessels ergibt sich aus der Tatsache, dass die Kommunikationspartner ihn selbst konstruieren muessen. Dabei wird eine oeffentlich zugaengige Datenquelle angezapft (am besten ein Satellit), die eine Folge von Zufallszahlen ausstrahlt. Man stellt die Sendestaerke so ein, dass der Empfang auf der Erde auch mit einer riesigen Antenne fehlerbehaftet ist. Der Sender (S), Empfaenger (E) und ein Aussenstehender, der die gleiche Datenquelle anzapft und die ganze Kommunikation zwischen S und E abhoert, empfangen zur gleichen Zeit unterschiedliche Folgen von Zufallszahlen. E und S teilen die empfangenen Folgen in Zweierpakete und errechnen von jedem Paket den Exclusive-Operations-Research-Wert (XOR-Wert). Die XOR-Operation macht aus zwei gleichen Zahlen eine 0 und aus zwei unterschiedlichen eine 1. Das ergibt eine neue Folge, die pro urspruenglich empfangenem Zweierblock nur noch eine Ziffer hat. Die neuen Folgen werden durch Kommunikation von E und S verglichen und auf Uebereinstimmung ueberprueft. So erhaelt man immer kuerzere Zahlenfolgen, die sich immer aehnlicher werden. Am Schluss stimmen die Resultate, die E und S getrennt an ihrem Standort berechnen, exakt ueberein.

20/7/22 (Item 9 from file: 95)
DIALOG(R)File 95:TEME-Technology & Management

00834996 I94112307273
Method for constructing a group-oriented cipher system
(Methode zur Bildung eines gruppenorientierten Verschluesselungssystems)
Chu-Hsing Lin; Chin-Chen Chang
Dept. of Comput. & Inf. Sci., Tung Hai Univ., Taichung, Taiwan
Computer Communications, v17, n11, pp805-808, 1994
Document type: journal article Language: English
Record type: Abstract
ISSN: 0140-3664

ABSTRACT:
In this research note, we propose a solution to the problem of generalized group-oriented cryptography. By applying the scheme presented one can send a confidential message to a group of users such that the message can be revealed only when the specified members cooperatively work together. The organization and policy of the target group does not need to be known by the **sender** ; only the public **keys** of **users** in the group are needed. The scheme presented is quite practical, and can be used in a large group-oriented network.

20/7/23 (Item 10 from file: 95)
DIALOG(R)File 95:TEME-Technology & Management

00627187 I92091591928
The digital signature standard proposed by NIST
(Der 'Digital Signatur Algorithm' von NIST)
anonym
Communications of the ACM, v35, n7, pp36-40, 1992
Document type: journal article Language: English
Record type: Abstract
ISSN: 0001-0782

ABSTRACT:
This standard specifies a Digital Signature Algorithm (DSA) appropriate for applications requiring a digital rather than written signature. The DSA digital signature is a pair of large numbers represented in a computer as strings of binary digits. The digital signature is a computer using a set of rules (i.e. the DSA) and a set of parameters enabling it to be used to verify the identity of the originator and integrity of the data. The DSA includes signature generation and verification. Generation makes use of a private key to generate a digital signature. Verification of the signature makes use of a public key that corresponds to, but is not the same as, the private key used to generate the signature. Each user possesses a private and public key pair. This standard is applicable to all federal departments and agencies for the protection of unclassified information. The article summarises the NIST proposal, discussing: the specifications for a DSS; use of the DSA algorithm; DSA parameters; and signature generation and verification. Appendices concern: a proof that v=r'; generation of parameters for the DSA; random number generation for the DSA, and modular arithmetic for the DSA.

20/7/24 (Item 1 from file: 99)
DIALOG(R)File 99:Wilson Appl. Sci & Tech Abs

1713591 H.W. WILSON RECORD NUMBER: BAST94063663
The keys to encryption
Riley, W. D;
Datamation v. 40 (Oct. 15 '94) p. 38
DOCUMENT TYPE: Feature Article ISSN: 0011-6963

ABSTRACT: Pretty Good Privacy (PGP), an encryption software system from Phil's Pretty Good Software, a company run by Philip Zimmermann, is so secure that the American government will not allow it to be exported. The software generates 2 passwords, or keys, for each person using it. The first key is public and known by all; the second key is private and known only by the user. Both keys are needed to code and decode a message. The **recipient** of an **encoded message** can authenticate the message sender's signature by decoding the message using the **sender** 's public, published **key** . The **recipient** can only read the message if the **keys** match. The **sender** of a private **message** would **encode** the **message** using the **recipient** 's public, published key. The recipient would then decode the message with his or her private key. Brief information on obtaining PGP is provided.

20/7/25 (Item 2 from file: 99)
DIALOG(R)File 99:Wilson Appl. Sci & Tech Abs

1402732 H.W. WILSON RECORD NUMBER: BAST96043134
Public key cryptography
Garfinkel, Simson L;
Computer v. 29 (June '96) p. 101-4
DOCUMENT TYPE: Feature Article ISSN: 0018-9162

ABSTRACT: Public key cryptography and factors that have delayed its mainstream acceptance are discussed. After much refinement from the initial concept, a public key cryptography system known as RSA is now available. With RSA, a public and a private key are created and anything encrypted with the public key can only be deciphered with the private key, thereby making it ideal for E-mail systems. In this case, the public **key** is **transmitted** over open channels, such as the Internet, and then used by the **receiver** to **encrypt** a **message** and transmit it back to the sender, who decrypts it with the private key. However, 3 factors have combined to delay the spread of public key cryptography. These are the speed difference between low-end and high-end computers, intellectual property law, and the U.S. government's export control laws. These issues are discussed.

20/7/26 (Item 1 from file: 144)
DIALOG(R)File 144:Pascal

12920406 PASCAL No.: 97-0188930
Blind decoding, blind undeniable signatures, and their applications to privacy protection
Information hiding : Cambridge, May 30 - June 1, 1996
SAKURAI K; YAMANE Y
ANDERSON Ross, ed
Dept. of Computer Science and Communication Engineering, Kyushu University, 812-81, Japan
Information hiding. International workshop, 1 (Cambridge GBR) 1996-05-30
Journal: Lecture notes in computer science, 1996, 1174 257-264
ISSN: 0302-9743 Availability: INIST-16343; 354000064017400180
No. of Refs.: 17 ref.
Document Type: P (Serial); C (Conference Proceedings) ; A (Analytic)
Country of Publication: Germany; United States
Language: English

A cryptographic concept, blind decoding is discussed: a **client** has a **message encrypted** with a server's public key and the client asks the server to decode the message without revealing what is the decoded plaintext nor learning the server's secret key. Blind decoding is a useful tool for protecting user's privacy in on-line shopping over the Internet. The RSA-based blind decoding is easily converted from the similar protocol as the Chaum's blind signature scheme, and a blind decoding protocol for the ElGamal encryption scheme is newly proposed. Moreover, the practical gap between the known RSA-based blind decoding and our ElGamal-based scheme is discussed in the application to protecting copyright matter of electronic documents. In blind decoding scheme, undetectability of the decrypted message has both negative and positive aspects: a negative aspect is considered as the problem of spotting the oracle and a positive aspect is applicable to making undeniable signatures blind against the signer.

20/7/27 (Item 1 from file: 202)
DIALOG(R)File 202:Info. Sci. & Tech. Abs.

3100907
Personal key archive.
Author(s): Linehan, M H; Simichich, N.J.; Tsudik, G.Y.
Patent Number(s): US 5495533
Publication Date: Feb 27, 1996
Language: English
Document Type: Patent
Record Type: Abstract
Journal Announcement: 3100

A computing system is described having an automated management system for managing keys to **encrypt** and decrypt stored **data** on the computing system. The computing system has an authentication server; a key client; a key generator; a key server; a key database; and an **encrypted data file** memory. The authentication server authenticates the user and in response to the user accessing the computing system the authentication server provides the user with a ticket validating the user. The key client of a creating user when creating a data file invokes the generator to generate a key corresponding to the data file. The key is provided to the key server and the key client uses the key to **encrypt** the **data file** which is stored in the **encrypted data file** memory. The key **client** of an accessing user sends its ticket and data file identification data to the key server. The key server checks the ticket and **sends** the **key** corresponding to the data file to the key client of the accessing user. The key client of the accessing user uses the key to decrypt the **encrypted data file** . The stored data can further include a header containing the key and owner and permitted user identification data. The ticket can contain a **key** to **encrypt messages sent** between the **client** server and key client.

20/7/28 (Item 2 from file: 202)
DIALOG(R)File 202:Info. Sci. & Tech. Abs.

2803006
Information distribution system.
Author(s): Lipscomb, T H; Sprague, P.J.
Patent Number(s): US 5247575
Publication Date: Sep 21, 1993
Language: English
Document Type: Patent
Record Type: Abstract
Journal Announcement: 2800

An information distribution system provides information to a user, when the information corresponds to criteria individually selected by the user, and then charges the user only for the selected **information** thus provided. **Encrypted information** packages (IP's) are provided at the user site, via high and/or low density storage media and/or by broadcast transmission. The IP's selected by the user are decrypted and then printed or displayed for viewing by the user. The charges for the IP's thus displayed are accumulated within the user apparatus and periodically reported by telephone to the system's central accounting facility which

issues encryption keys. The encryption keys, used to decrypt the IP's, are changed periodically. If the central accounting facility has not **issued** a new encryption **key** for a particular **user** station, the station is unable to retrieve information from the system when the key is changed.

20/7/29 (Item 1 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00486326 98WN02-031
Your own private Internet -- Virtual private networks expand your LAN across the Internet and make high-speed, low-cost remote access a reality - without...
Hafke, David
Windows Magazine , February 1, 1998 , v9 n2 p218-226, 6 Page(s)
ISSN: 060-1066
Focuses on virtual private networks (VPNs), noting that they provide a secure gateway between user's LAN and the Internet by means of a local phone call to an Internet service provider. Indicates that VPNs let remote users take full advantage of whatever high-speed connections they have installed locally. Covers various types of VPNs, including Microsoft's Point-to-Point Tunneling Protocol, which grabs a PPP packet from the **client** or server, then **encodes** the **data** with a 40-bit RSA RC4 encryption **key** before **sending** any data. Also describes IPsec, which provides a high degree of security, and SOCKS, a circuit-level proxy for handling encryption and authentication between two networks. Suggests that if user's main concern in a VPN is price, the included PPTP support in Win95 and NT is a good choice, that IPsec is not yet standardized, and that SOCKS is a ratified IEFT standard, but can be quite expensive. Includes one sidebar, one table, one diagram, and a product source guide. (jo)

20/7/30 (Item 2 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00453758 97BY03-014
Digital IDs -- Server and client certificates aren't yet widely used for authentication, but that's changing fast. Here's a progress report
Udell, Jon
BYTE , March 1, 1997 , v22 n3 p115-118, 3 Page(s)
ISSN: 0360-5280
Contends that digital forms of identification will be the best way to regulate access to subscriber-only areas of the BYTE Site. Provides a discussion of the author's experiments with digital IDs to secure a Web server, authenticate Web clients, and sign and encrypt e-mail. Explains that, in order to establish Secure Sockets Layer sessions with browsers, a Web server needs to hold a digital server certificate. Says that this has the public key that the browser fetches to it, so that it can **encrypt messages** and send them back to the server. Specifies that to acquire a certificate, **users** must generate a **key** pair before **sending** the request file by e-mail, receive, and then install the signed certificate. Focuses on reciprocal authentication; Sioux authentication, which exports the fields of a client certificate as Common Gateway Interface variables; and authentication with IIS. Includes one diagram and one sidebar. (jo)

20/7/31 (Item 3 from file: 233)
DIALOG(R)File 233:Internet & Personal Comp. Abs.

00429338 96MF07-003

ViaCrypt PGP offers easy corporate security

Burger, Doug

Mobile Office , July 1, 1996 , v7 n7 p20, 1 Page(s)
ISSN: 1047-1952
Company Name: ViaCrypt
Product Name: ViaCrypt PGP Business Edition

Presents a very favorable review of ViaCrypt PGP Business Edition v4.0 ($149, single user; $450, five users; $1,340, 20 users; corporate bundles available), encryption software from ViaCrypt Corp. of Phoenix, AZ (800). Reports that it is available for several platforms including Windows, DOS, Mac, and Unix. States that the company has exclusive commercial rights to the PGP (Pretty Good Privacy) code, and it uses the Rivest-Shamir-Adelman (RSA) public key system. Says it is remarkably easy to use, and it provides many features for business convenience. Complains that you must obtain the **recipient** 's public **key** in order to **send** **encrypted** **data** , although the product has a convenient key management system. Concludes that this software should fulfill the security needs of most users. Includes one screen display. (bjp)

?